Smart City, Internet of Things, Security and Privacy

Peter Waher

Abstract. This course contains a series of lectures and practical laboratory assignments spanning four days that provide the participants with the fundamental ideas, visions and the technologies related to the development of services for the Smart City (or Society) and the Internet of Things. At the end of the course, the participant will have sufficient knowledge to have a general overview of the area, awareness of big movements within the industry, ability to make decisions of architectural importance, avoiding the largest pitfalls and protect the rights of all users. The course is aimed at computer science undergraduate or graduate students, as well as engineers in related areas.

Keywords: Smart City, Internet of Things, IoT, Cyber-Physical Systems, CPS, Security, Privacy, HTTP, MQTT, CoAP, LWM2M, XMPP, Block-Chain, Interoperability, GDPR.

1 First day: Connectivity and Interoperability

The first day is focused on the presentation of basic definitions and introduction to fundamental technologies. The day concludes with a comparison of the different technologies, with the goal of giving an understanding for what type of applications each one is suitable for. Focus for the first day is connectivity, or how to connect things to the Internet.

1.1 09:00-09.45: Vision of the Smart City

We begin with an introduction of the concept of the Smart City and how it is related to other related fields such as Internet of Things and Cyber-Physical Systems. Focus lies with presenting definitions that result in rewarding areas of study.

1.2 10:00-10.45: Web of Things

The HTTP protocol is probably the most known protocol among developers and users in the world. The lecture shows how it can be used for the Internet of Things, its pros and its cons.

1.3 11:00-11.45: Publish/Subscribe

The communication pattern Publish/Subscribe has become the most popular communication pattern in the world for use with Internet of Things. In this presentation we analyze the reasons for this, as well as its pros and cons. We also introduce the protocol MQTT.

1.4 12:00-12.45: Resource-constrained Devices

In Cyber-Physical Systems there are devices with different characteristics. Some are powerful, others have restrictions on its processing or communication resources. Regardless if the restrictions are related to processing power (CPU or memory) or network band-width, there often exists a necessity to be able to communicate in a simple and efficient manner. The CoAP (Constrained Application Protocol) was developed for this purpose. The presentation gives an introduction to this protocol and analyzes its pros and cons.

1.5 13:00-14.30: Lunch

Time for recharging batteries.

1.6 14:30-15.15: Interoperability

Each standard tries to create a layer of interoperability between actors. Each of the presented protocols is an example of a standard within the area of communication. Within the area of Internet of Tings, there exist standards that reach all the way to the application layer, in the OSI model. This allows users to interchange equipment, infrastructure and systems, something that will boost the technology and the companies that adopt such technologies. This presentation focuses on the standards Light-Weight Machine-to-Machine (LWM2M) and IPSO Smart Objects, as first examples of standards that reach the application level.

1.7 15:30-16.15: Decentralization and federation

To realize global solutions, you need a strategy for scalability made from the start. Scalability normally depends on the technologies used. Changing technologies later, once solutions have been published, can be very difficult. For this reason, it’s important to choose a technology already on the onset, that supports the supposed necessities envisioned from the start. The lecture introduces key concepts on how to reach global scalability: Decentralization and federation. It also introduces the eXtensible Messaging and Presence Protocol (XMPP), which permits global communication, while at the same time solving the problems of topology, distribution and interoperability on the Internet.

1.8 16:30-17:00: Summary

The day ends with a summary of the protocols presented and a comparison between them.

2 Second day: Security, Privacy and Provisioning

With the basic knowledge of how to connect devices to the Internet, the second day focuses on practical problems on how to maintain, administer and configure systems in the network. It also analyzes new requirements of privacy that appear in legislation in different parts of the world, and how it affects our information systems.

2.1 09:00-09.45: The Internet

The Internet is not the same place as protected internal network. Developing services for the Internet is not the same thing as developing services for use in internal networks. Furthermore, systems for the Internet of Things are also different to traditional systems: They consist of many distributed nodes that are often without supervision of natural human beings for long periods of time. The lecture introduces various security aspects related to the Internet of Things with the goal of raising the awareness of risks of poor security for Cyber-Physical Systems.

2.2 10:00-10.45: Ubiquitous encryption

To obtain a minimum level of security for systems working on the Internet, especially if the process personal or sensitive information, encryption is required. Today, there are few reasons not to use it. This presentation introduces the basic concepts related to security on the Internet, such as encryption, authentication, authorization, end-to-end encryption, using hash functions instead of passwords with the goal of realizing systems that support the vision of ubiquitous encryption.

2.3 11:00-11.45: Privacy

Privacy is a fundamental human right. In this lecture you are presented with what this right consists of, and why it is important. The lecture also introduces some of the new legislation regarding privacy, such as the GDPR, and what it implies for developers of information systems that process personal information, and why this is important for Internet of Things systems and the Smart City.

2.4 12:00-12.45: Data Protection by design and by default

There are many methods to protect sensitive and private data, more than just encryption of data in transit or at rest. Much depends on the architecture and design of the system. The new laws protecting privacy require data protection to be done “by

design and by default". This lecture will be focused on analyzing basic design methods you can use to better protect information, such as decentralization, anonymization, pseudonymization, obfuscation, data masking, data aggregation, event logs and monitoring. It also analyzes what it means to protect data by default.

2.5 13:00-14.30: Lunch

Time for recharging batteries.

2.6 14:30-15.15: Discovery of devices

The natural instinct when you create secure systems on the Internet is to close access to components to everyone except a few predetermined persons. Such a strategy can be counter-productive if you want to realize interoperable systems for the Smart City. This lecture presents a method to publish the presence of things in interoperable Thing Registries. These registries permit things to find other things, forming *ad hoc* networks on the Internet, without requiring administration or configuration of the networks on part of the operators ("zero configuration").

2.7 15:30-16.15: Provisioning and the Life Cycle of things

Without a way to control who can access what things, and do what with them, *ad hoc* networks are insecure. This lecture presents a method of interoperable provisioning that avoids placing responsibility on the operators for controlling access rights. The concept of ownership, and a method that permits the owner to control the access rights of its things in the network is introduced. The network learns from what the owner wants, to form an autonomous, secure, but at the same time open and interoperable network.

2.8 16:30-17.15: IoT Harmonization and economic feedback

In order to realize a Smart City, it is not sufficient to create open, secure and interoperable *ad hoc* networks of things, even though that is an important step. The vision of the Smart City requires owners of things to make them available to others, so that they can reuse them for other purposes than the original one. It is necessary to have an exchange of information and things in order to have cross-fertilization between different domains of life. To realize this, you need a mode of economic feedback based on access and usage of data in the network. This lecture presents an effort within the IEEE that has this goal: "IoT Harmonization".

2.9 17:30-18:00: Summary

The day ends with a summary of the ideas presented.

3 Third day: Practical labs, Connectivity

The third and fourth days are dedicated to practical labs. On the third day, the participants form groups with the goal of realizing interoperable sensors, actuators and controllers using Raspberry Pi and development using .NET. Example code and hardware will be available. The course follows the presentation and examples available in the book “Mastering Internet of Things” by Peter Waher.

3.1 09:00-10:45: Sensors and actuators

In the first lab, we assemble a sensor and an actuator utilizing Raspberry Pi and Arduino. We learn how to use Windows 10 for IoT and use the most common tools.

3.2 11:00-12:45: Communication using MQTT

The MQTT protocol is the easiest protocol to begin using to distribute information in IoT. In this lab we use MQTT to publish data from sensors and send commands from controllers to actuators.

3.3 13:00-14.30: Lunch

Time for recharging batteries.

14:30-17:00: Communication using HTTP

HTTP is the most known protocol, its popular and versatile. We use HTTP in this lab as a means to see how we can publish sensor data, control actuators and easily publish human interfaces for our things.

4 Fourth day: Practical labs, Interoperability

The fourth day is dedicated to practical labs related to interoperability. We continue with the sensors and actuators created during the previous day.

4.1 09:00-10:45: Communication using CoAP and LWM2M

Knowing HTTP, it is easy to start using CoAP. We use CoAP to create more efficient interfaces for our sensors and actuators. We also add a layer of interoperability using LWM2M.

4.2 11:00-12:45: Communication using XMPP

The XMPP protocol is the most potent of all the protocols presented. In this lab we introduce XMPP in order for the participant to learn some of the more basic possibilities the protocol gives for the IoT.

4.3 13:00-14.30: Lunch

Time for recharging batteries.

14:30-15:15: Discovery of things

We continue with the XMPP lab, introducing Thing Registries and how they can be used for discovery of things in the network based on their properties and characteristics.

15:30-17:00: The controller

We continue the XMPP lab by developing a controller. The controller will automatically discover our sensors and actuators registered in the Thing Registry. It will control the actuator of it choice based on data made available by the sensor of its choice, in real-time.

If time permits: Provisioning

For groups finishing their labs quicker than the allotted time, there exists an opportunity to broaden the last labs, including provisioning as a layer of security. Provisioning permits the owner of a thing to control who can connect with its devices and do what with them.

For those that do not have time to finish the goals of each lab, there exists an opportunity to finish them in your own spare time and communicate with the author using electronic means.