

Project Acronym and Title:

5GhOSTS - 5TH GENERATION SECURITY FOR TELECOM SERVICES

Deliverable:

D4.4: REPORT ON LOCAL AND NETWORK ACTIVITIES

Authors and affiliation:

Eddy Truyen (KU Leuven), Christoph Baumann (EAB), Jan Tobias Mühlberg (KU Leuven), Vlasios Tsiatsis (EAB)

Eddy.Truyen@cs.kuleuven.be, Christoph.Baumann@ericsson.com, JanTobias.Muehlberg@cs.kuleuven.be, Vlasios.Tsiatsis@ericsson.com

D4.4 Revision: 1.1



This report is part of a project that has received funding by the *European Union's Horizon 2020 research and innovation programme* under grant agreement number 814035. The content of this report reflects only the authors' view. The *Innovation and Networks Executive Agency (INEA)* is not responsible for any use that may be made of the information it contains.

 Copyright © 5GhOSTS Consortium 2019-2023

Project funded by the European Commission within the Horizon 2020 Programme **Dissemination Level**		
PU	Public	X
CO	Confidential, only for members of the consortium (incl. the Commission Services)	
CL	Classified, as referred to in Commission decision 2001/844/EC	

Deliverable number:	4.4
Deliverable name:	Report on Local and Network Activities
Work package:	4
Lead WP / Deliverable beneficiary:	KU LEUVEN

Status of deliverable		
	By	**Date**
Submitted (Author(s))	Eddy Truyen	2021-09-24
Verified (WP leader)	Jan Tobias Mühlberg	2021-09-27
Approved (PMB member)	Hans Eriksson	2021-09-29
Approved (Coordinator)	Jan Tobias Mühlberg	2021-09-30

Author(s)		
Name	**Organisation**	**E-mail**
Eddy Truyen	KU LEUVEN	eddy.truyen@cs.kuleuven.be
Christoph Baumann	EAB	christoph.baumann@ericsson.com
Jan Tobias Muehlberg	KU LEUVEN	jantobias.muehlberg@cs.kuleuven.be
Peggy Valcke	KU LEUVEN	peggy.valcke@kuleuven.be
Vlasios Tsiatsis	EAB	vlasios.tsiatsis@ericsson.com

Copyright © 5GhOSTS Consortium 2019-2023

Public introduction
5GhOSTS will analyze and improve the security of service-based implementations of 5G networks, relevant to protect the EU's critical communication infrastructure. Starting from the emerging 3GPP's service-based architecture for 5G networks, which includes virtualization of mobile and core network functions, the project aims to improve the security of virtualization technologies: containers, lightweight Virtual Machines and orchestration frameworks. Unlike previous evolutions in the telecommunications sector, the 5th Generation of Telecommunication Systems (5G) presents diverse and novel requirements for technologies such as heterogeneous air interfaces, Software Defined Networking, Network Functions Virtualization, Mobile Edge Computing and Fog Computing, as well as algorithms to optimize the management of such complex networks. As a result, the 5G evolution will mainly built on layers of software services. The telecom industry is migrating to virtualized and orchestrated environments, allowing the deployment of Virtual Network Functions (VNFs) on cloud infrastructure enabling the concept of network slicing. The main motivation driver for this move is sustainability through cost and energy reduction as well as full automation of telecom systems operations facilitating dynamic and scalable adaptation to service demands. State-of-the-art light-weight virtualization and container orchestration frameworks clearly contribute to this driver, but do not meet the stringent security requirements of telecommunication systems.

Executive Report Summary
This deliverable presents an overview of the training activities organized by the 5GhOSTS project members during the period September 2019 until August 2021.

 Copyright © 5GhOSTS Consortium 2019-2023

Table of Contents

Table of Contents 4
Introduction 5
1. Training program 5
1.1 Objectives of the training program (EID) 5
1.2 Innovative aspects of the training program 5
1.3 Content structure 6
1.4 Supervision arrangements 6
2. Deviations to the planning due to the Corona crisis and recruitment delay 7
3. Overview of network-wide training activities 10
3.1 Intensive course on computer-aided verification of security properties of software systems 10
3.2 Hands-on course with containers/light-weight VMs platforms and container orchestration frameworks 11
3.3 Intensive course on edge networks, in particular IoT and telecommunication Part I 13
3.4 Intellectual Property Rights (IPR) training 14
3.5. Industry-oriented conference attendance 15
4. Local trainings 16
4.1 ESR1 16
4.2 ESR2 17
4.3 ESR3 17
4.4 ESR4 18

Copyright © 5GhOSTS Consortium 2019-2023

Introduction

This document presents an overview of the training activities of the 5GhOSTS program during the first 24 months of the project. It presents both local and network-wide activities.

The 5GhOSTS project aims to improve the security of container-based platforms in the edge of 5G networks. Mobile edge computing (MEC) plays a central role in 5G networks to achieve ultra-low latency and ultra-reliability requirements of the envisioned 5G applications. Services are deployed on demand, replicated and scaled across distributed edge clouds that are in the proximity of the radio base stations. By relying on container-based orchestration, virtual network functions (VNFs) are to be dynamically instantiated across such distributed edge clouds.

Kubernetes is the de-facto standard for deploying and managing cloud-native applications on top of portable container-based clusters that can run anywhere. Kubernetes has also been put forward as the foundation for deploying VNFs in distributed edge clouds of the 5G network.

To increase the security of Kubernetes without lowering its performance, 5GhOSTS is creating novel building blocks for increasing the confidentiality and integrity of container image repositories, container runtimes, the Kubernetes orchestration framework itself and the container network. These building blocks are based on well-founded methods such as trusted computing, secure programming languages and formal verification. Moreover, 5GhOSTS also conducts legal research with a focus on privacy in the context of telecommunication law so that the building blocks are engineered with privacy in mind.

1. Training program

1.1 Objectives of the training program (EID)

The 5GhOSTS training objectives are twofold:

1. To form an ***international and interdisciplinary research group*** of 4 ESRs and senior researchers from academia and industry. The ESRs will benefit from close intersectoral collaboration to develop transferable skills, both soft and technical skills that will uplift their future careers. The ambitious training network leverages academic excellence and intersectoral mobility, together with a ***strong business- and innovation-oriented mind-set***, to develop technical skills with a thorough understanding of legal and business aspects of the telecommunication industry. 5GhOSTS fosters thus **innovation and standardization in the mobile networks of the future**, focusing on security and privacy in an EU context
2. To address the growing need of the ***EU economy*** for young researchers with a strong profile (technical, legal and economic) in the 5G telecommunications domain, thus increasing the research ***international competitiveness***.

5GhOSTS is led by 2 beneficiaries: Ericsson is a global company at the forefront of communications technology and 5G Telecom System. Ericsson has an extensive experience in participating in Standards Development Organizations (SDOs), actively contributing to standards specifications as well as providing excellent training in a range of advanced research and transferrable skills aligned to the exploitation of the research results of 5GhOSTS. KU Leuven has extensive experience in virtualization technology, middleware, privacy, formal software development, trusted computing and ICT & media law. Finally, secappdev.org is participating as a partner organization to provide training and networking opportunities with a focus on software security.

1.2 Innovative aspects of the training program

We believe the 5GhOSTS training program is innovative in Europe because of the following reasons:

 Copyright © 5GhOSTS Consortium 2019-2023

- The **innovative aspects of research activities** to be conducted by ESRs.
- The training program takes an **interdisciplinary approach** (involving economic, social and legal domains) that will be sustained by several activities at local, network-wide and external level.
- 5GhOSTS pays specific attention to **standardization.** The project training includes activities that involve the ESRs in working closely together with experienced standardization professionals and training them in the practices of relevant standardization organizations such as 3GPP and ETSI. Trainings at different international departments of Ericsson (Stockholm, Lund, Jorvas), who are specialized in specific standardization sub-areas, will also be organized
- A special focus will be on introducing the ESRs to the principles of **Open Innovation, Open Science and Open to the World**[1] mainly through participation to specialized on-line courses, specific thematic courses organized by KU Leuven, and direct experience with open access publishing platforms and research data management platforms.
- An alignment of the training courses with the **Sustainable Development knowledge platform**[2] - with respect to *Sustainable Development Goals (SDGs) 9, 8 and 5 – "Resilient infrastructure", "Full and productive employment" and "Gender equality"* – will open the mindset of the ESRs towards the entire world, including entrepreneurial activities in the development countries.

1.3 Content structure

To meet the aforementioned training objectives, we provide training in three skill areas (SAs)**: Specific research skills, advanced telecom R&D skills, and transferable skills**. To meet the research objectives, the technical trainings logically focus on the intersection of Kubernetes, Security and Mobile Edge Computing in 5G networks. These technical trainings are complemented with trainings on IPR management, standardization of telecommunication systems, and legal training on telecommunication law. Transferable skills trainings include a component on Open Science principles, methods and tools. Such training and on-line tools with respect to open science are delivered by KU Leuven's Research Coordination Office. We also include a number of on-line assets offered by external organizations such as Foster, OpenAire, etc. (see bottom of Table 1.2.c). Moreover, courses on entrepreneurship and exploitation are provided by KU Leuven's R&D Tech Transfer Office. Trainings on all other transferrable skills are coordinated by KU Leuven's YouReCa (Young Researchers' Career) center and most of them are delivered by the KU Leuven's HR department. Ericsson complements by hands-on training and highly-referenced MOOCs on project management. In addition, the ESRs will also be trained through a hands-on-approach: after an initial formal training, they will be involved in project reporting and in the organisation of project meetings, dissemination events and the organization of the SecAppDev course.

1.4 Supervision arrangements

The research training will be delivered to the 4 ESRs undertaking collaborative research projects towards a PhD degree: All ESRs will be enrolled in the doctoral programme of KU Leuven. For ESR1-3, the regulations, guidelines and progress monitoring instruments for the ESRs are those of KU Leuven's Arenberg doctoral school programme[3]. For ESR4, the regulations, guidelines and progress monitoring instruments for the ESRs are those of KU Leuven's Faculty of Law[4].

[1] https://ec.europa.eu/research/openscience/index.cfm
[2] https://ec.europa.eu/info/strategy/international-strategies/global-topics/sustainable-development-goals/eu-approach-sustainable-development_en , https://sustainabledevelopment.un.org/
[3] https://admin.kuleuven.be/rd/doctoraatsreglement/en/phdregulation-st
[4] https://www.law.kuleuven.be/faculty/PhDwebsite

Copyright © 5GhOSTS Consortium 2019-2023

ESRs will each benefit of the supervision of an interdisciplinary Supervisory Team composed of a lead Supervisor (from the host beneficiary and with expertise in the specific field of the individual research project) and by 4 co-supervisors partly from other disciplines. For the ESR with technical topics in Computer Sciences the co-supervisors involve one person with an understanding of business processes on the Telecom sector, one co-supervisor who specialises on privacy and ICT law, and one secondary technical supervisor. For the ESR with a focus on privacy law, the main supervisor is a law researcher and thus the co-supervisors are from technical fields. The Supervisory Team will guarantee that acquired skills are actually interdisciplinary and address industrial needs.

2. Deviations to the planning due to the Corona crisis and recruitment delay

For both network-wide and local trainings the initial plan was that ESRs do not travel to attend remote trainings, but trainings are repeated whenever two ESRs are scheduled to reside at the local training site and have not yet followed that training.

As a result of the COVID-19 pandemic, all secondments have been postponed in the first half of the project. All trainings are organized in a virtual format so that all ESRs can attend at once.

No trainings have been cancelled, except the SecAppDev course in 2020 and 2021 because the essential characteristic of the course week depends on all participants and lectures being physically together. To account for this loss, alternative summer schools have been collected (see Table 1). Now that the force of the pandemic has weakened, SecAppDev 2022 will take place in March 2022 and all ESRs will participate in in SecAppDev and will also be active in the local organization of the course week in order to learn conference organization skills.

Table 1. Alternatives to the SecAppDev course week in 2021

Name	Date	Online / Physical	Link
Seminar in Information Security & Cryptography	June 14-16, 2021	Physical, Zurich Switzerland	https://www.infsec.ch/seminar2021.html
Cyber Security and Privacy (CySeP) Summer School	TBA (canceled in 2020)	TBA, Stockholm Sweden	https://cysep.conf.kth.se/
Marktoberdorf Summer School: Engineering Secure and Dependable Software Systems	TBA (canceled in 2020)	TBA, Marktoberdorf Germany	https://i4.pages.gitlab.lrz.de/organization/mod-2020/

 Copyright © 5GhOSTS Consortium 2019-2023

Cyber Security Summer School	July 04-24, 2021	Zagred, Zadar, Croatia	https://www.algebra.hr/international-school/summer-school/courses/cyber-security/
Summer School on Formal Techniques	May 22-28, 2021	Online	http://fm.csl.sri.com/SSFT21/
SICT Summer School on Sustainable ICT	August 30 – September 3rd, 2021	Louvain-la-Neuve, BE	https://sites.uclouvain.be/sict/

There was also a recruitment delay for the positions of ESR1 and ESR3. As a result, all trainings at the Ericsson side have been postponed until the recruitment phase has been fully completed

Below, the interested reader can find an overview of planning deviations. For each phase of the project, the original planning of the grant agreement is presented, thereafter modifications to the planning are presented. Note that at the time of writing this report, Ericcson has still a ban on all business travel. For KU Leuven employees, there is no longer a travel ban but business travel had been discouraged throughout an extended duration.

- First phase from M6 (Feb 2020) to M9 (May 2020)
    - Original planning: ESR2 and ESR4 start at their home institution to follow intensive courses on container platforms at KUL, part I of the intensive course on computer-aided verification of security properties (system-security), and the SecAppDev course week in 2020.
    - Deviations to planning:
        - SecAppDev 2020 has been cancelled due to the outbreak of the COVID-19 virus and the subsequent full-lockdown in Belgium.
        - The internal course on systems security had been delayed to enable all ESRs to participate.
        - ESR2 followed the entire course on container platforms as planned, because the course shifted from a physical to a virtual format.
        - ESR4 took the initiative to follow introductory courses on ICT on-line. These courses were better suited for ESR4 as he has a master in Law and not in computer science. The courses have been homologated by the Joint Supervisory Board as a replacement for the course on container platforms
- Second phase from M10 (June 2020) until M13 (September 2020)
    - Original planning: ESR1 and ES3 start their contract. ESR1 and ESR3 follow the Edge & IoT technology for telecom training and the IPR training at Ericsson. They will also attend Part II of the course on computer-aided verification of security properties (formal methods).
    - Deviations to planning: All trainings by Ericsson were postponed due to a recruitment delay and the COVID-19 pandemic.
- Third phase, from M14 (October 2020) to M19(March 2021)
    - Original planning: All ESRs stay at Ericsson. During this phase, all ESRs will attend standardization training, take business modelling courses and learn how to derive commercially exploitable products by working with professionals at Ericsson Stockholm and follow training on IPR management; ESR1 and ESR3 will follow part I of the intensive

Copyright © 5GhOSTS Consortium 2019-2023

course on computer-aided verification of security properties (system security), and the SecAppDev course week in 2021.

- Deviations to planning:
  - SecAppDev 2021 was also cancelled due to COVID-19. Alternative summer schools have been collected (see Table 1)
  - Part I of the security course, which was originally planned during the first phase has been organized during M10. All four ESRs attended.
  - The standardization training and business modelling courses at Ericsson have been postponed due to the late recruitment of ESR1 and ESR3. Initial concepts on standardization were taught by means of an on-line lecture (for which the ESRs were invited by the ITN-project HEART).
  - The training on IPR management by Ericsson started in M19 in a virtual format, was preceded by a general lecture on IPR concepts by KU Leuven and was followed up in M22 with a patent creation exercise.
  - Finally a 4 hour session to teach hands-on experience with Kubernetes to ESR1 and ESR3 was organized in M16.

- Fourth phase from M20 (April 2021) until M24 (August 2021)
  - Original planning: ESR1 and ESR3 stay at KU Leuven and will follow the intensive course on container platforms. Additionally ESR2 and ESR4 will work with standardization professionals from Jorvas (FI) on learning how to transfer privacy results.
  - Deviations to planning:
    - The training on container platforms took place a second time in a virtual format. ESR1 and ESR3 both attended.
    - Part II of the security training on formal methods has taken a custom approach where each ESR will be offered specialized teaching materials (text books, on-line lectures, summer schools) that touch upon the expected tasks and outcomes of their respective project. ESR2 is learning about formal methods for verification of network policies in Kubernetes, whereas ESR1 and ESR3 will follow an on-line summer school on formal techniques[5].
    - ESR2 attended the KubeCon industry conference[6].
    - ESR2 also started to work with a business professional at Ericsson on the topic of hardening network policies in Kubernetes.
    - The postponed training on edge computing with a focus on telecommunication systems has been split in two parts. Part I has been held in M22 in a virtual format, whereas Part II will be held in M26.

Table 2 Overview of NETWORK-wide Training Events conducted during the period M1-M24

Main Training Events & Conferences	**Lead Institution**	**Action Month**
Intensive course on computer-aided verification of security properties of software systems	KU Leuven & Ericsson	M16/ M20-M21
Hands-on course with containers/light-weight VMs platforms and container orchestration frameworks	KU Leuven	M6-M8/ M16/ M18-M20
Intensive course on edge networks, in particular IoT and telecommunication Part I	Ericsson	M22

[5] http://fm.csl.sri.com/SSFT21/

[6] https://events.linuxfoundation.org/kubecon-cloudnativecon-europe/

 Copyright © 5GhOSTS Consortium 2019-2023

Intellectual Property Rights (IPR) training	Ericsson	M15,M20,M22
Industry-oriented conference attendance (one per ESR)	External	M24-M27

3. Overview of network-wide training activities

Table 2 provides an overview of the actually conducted network wide training events. All events have been conducted in a virtual format except the first three training sessions of the hands-on-course on Kubernetes. Some planned training events that could not be held in a virtual format have been rescheduled to the second half of the project.

3.1 Intensive course on computer-aided verification of security properties of software systems

The goal of the ESRs for this course are four-fold:

(i) To develop a good understanding of information security, its impact on/application in software development and the broader context of threats, vulnerabilities and risks in the ICT environment.

(ii) Understanding the different types of vulnerabilities in system software and learn techniques to automatically detect and prevent vulnerabilities in software

(iii) Grasp the concept of enclaves and acquire hands-on experience with trusted computing architectures such as Intel SGX, ARM TrustZone, and Sancus to develop enclaved software modules. Understand the challenges with interconnecting enclave applications in heterogeneous and distributed environments for secure-sensitive networked applications

(iv) Hands-on experience with so-called side-channels attacks that exploit vulnerabilities of the hardware itself.

The covered topics are:

I. Security in the Software Development Life-cycle:
   a. Making security part of the process during the design, development and deployment of systems
   b. Security assessment techniques that can be integrated in various stages throughout the SDLC;
   c. STRIDE (Spoofing identity, Tampering with data, Repudiation threats, Information disclosure, Denial of service and Elevation of privileges)
   d. Data flow diagrams and threat modelling

II. Security Policies and Mechanisms
   a. Sandboxing,
   b. Runtime monitoring
   c. Information flow control

III. Access Control and Authorisation
   a. Mandatory Access Control (MAC)
   b. Discretionary Access Control (DAC)
   c. Role-Based Access Control (RBAC)
   d. Access control implementation techniques

Copyright © 5GhOSTS Consortium 2019-2023

   e. An overview of challenges in modern systems
IV. Low-level Vulnerabilities in Software and Hardware
   a. Program execution on modern processors
   b. Buffer overflows on stack and heap
   c. Return-oriented programming
   d. Data-only attacks
   e. Side-channels
   f. Hardware vulnerabilities
V. Automated Detection and Prevention of Vulnerabilities in Software
   a. Penetration testing
   b. Automating penetration testing,
   c. Fuzz-testing
VI. Trusted computing
   a. Enclaves
   b. Trusted Computing and remote attestation
   c. Authentic Execution on heterogeneous Trusted Computing infrastructure
   d. Pitfalls: untrusted pointers, function pointers, resource sharing, debugging
   e. Compartmentalising applications
   f. Side-channels and how to avoid them
   g. Open research questions
VII. Exercises using a relevant case study of the 5GhOSTS project:
   a. Data flow diagram
   b. STRIDE analysis and Threat modelling
   c. Access Control and Authorization
VIII. Tutorial 1: Exploitation and Fuzzing by means of American Fuzzy Lop (AFL)
IX. Tutorial 2: Building Distributed Enclave Applications with Sancus and SGX

3.2 Hands-on course with containers/light-weight VMs platforms and container orchestration frameworks

The course on containers and container orchestration frameworks has run two times. It coincides with a module of the KU Leuven course Capita Selecta Distributed Systems[7] that is taught to the students in the program for Master in Computer Science. The first instance of the course has been followed by ESR2, whereas the second instance has been followed by ESR1 and ESR3. This second instance was preceded by a short course given to the ESR1 and ESR3 in order to compensate the delay of recruitment and give the ESRs as quickly as possible the necessary background.

The goal of the ESRs for this course is two-fold:

(i) Learn the concepts of Kubernetes in a systematic way so the students get an in-born navigation of the big picture, which is represented as a feature taxonomy consisting of 9 functional aspects.

(ii) Learn to use a few practical building blocks as part of an in-house developed on-line tutorial[8]

[7] https://onderwijsaanbod.kuleuven.be/syllabi/e/H04G7AE.htm

[8] https://github.com/k8-scalar/k8-scalar

 Copyright © 5GhOSTS Consortium 2019-2023

The covered topics are:

I. Cluster architecture and setup
   a. The declarative configuration management approach of Kubernetes
   b. The master control plane and its REST API
   c. Worker nodes
   d. Installation methods

II. Framework customization interfaces
   a. Feature gates
   b. Admission controllers
   c. Scheduler plugins
   d. Networking plugins
   e. Plugin-architecture for other container runtimes
   f. Storage volume plugins
   g. Identity and Access Management (IAM) modules
   h. Annotations
   i. Extending the main REST API with custom resource definitions (CRDs)
   j. Aggregation of new APIs
   k. Management of extended node resources such as GPU
   l. CloudControllerManager plugin
   m. The KubeletConfiguration API

III. Application configuration and deployment.
   a. Pods
   b. Reuse of modular Pod configuration fragments by means of PodPreset and ConfigMap resources.
   c. Workloads types: ReplicaSet, StatefulSet, DaemonSet, Jobs
   d. Horizontal and Vertical Pod Autoscalers.
   e. Different types of (rolling) update strategies for Pods.

IV. Services networking and load balancing
   a. Exposing the services of Pods through a stable network address that survives failures and migration of Pods: ClusterIP address, NodePort or cloud-provided external LoadBalancer
   b. The kube-proxy, a Layer 4 load balancer, runs on every node of the cluster to serve all ClusterIP and NodePort services.
   c. Headless services bypass the kube-proxy and expose each replicated Pod as a stable DNS name that is registered in the internal DNS server of the cluster.
   d. Ingress resources additionally declare HTTPS load balancer rules for the services that are exposed via a Cluster IP.
   e. Services of type ExternalName declare a DNS name for a depended service that does not run inside the k8s cluster.

V. Resource quota
   a. Multi-tenancy
   b. Namespaces
   c. Compute quota
   d. Object count quota

VI. Container QoS management
   a. Requests and Limits with support for oversubscription

Copyright © 5GhOSTS Consortium 2019-2023

   b. CPU management and Socket Topology for performance sensitive workloads
   c. Highly expressive Pod placement constraints
   d. Pre-emptive scheduling of Pods
   e. Handling of out-of-resource conditions of workers nodes by pro-active Pod eviction and reactive resource reclamation
   f. Pod priority

VII. Securing clusters:
   a. Identity and Access Management of the REST API and the Kubelet API
   b. Network encryption of control and application packets
   c. Network policies

VIII. Securing containers
   a. Improved security isolation of containers using SecurityContexts.
   b. Additional verification and enforcement of particular SecurityContexts upon Pods by means of PodSecurityPolicies (deprecated).

IX. Applications and cluster management
   a. The Kubernetes dashboard
   b. Central monitoring of container resource usage. Kubernetes distinguishes the core metrics server for auto-scaling of Pods and a third party full metrics pipeline backed-up by a time-series database.
   c. Central monitoring of resource usage of the Kubernetes platform itself
   d. Logging and debugging at the level of containers and integration with log aggregation systems.
   e. Cluster maintenance such as cluster software upgrades, dynamic reconfiguration of the kubelet without restarting Pods, draining of nodes, garbage collection of container and images and support for disruption budgets.
   f. Kubernetes clusters that runs across multiple zones or regions
   g. Kubernetes's federation API that allows managing clusters into a federation
   h. ServiceCatalog API

3.3 Intensive course on edge networks, in particular IoT and telecommunication Part I

This training aims to familiarize the ESRs with edge and cloud computing fundamentals, business considerations and use cases, as well as security and standardization aspects. The training is mainly based on internal Ericsson training material and is complemented by presentations from experts and some cloud management and orchestration exercises. The curriculum consists of two parts:

(i) Introduction and use cases: here we introduce the edge computing concept and benefits, the business model, actors and their relations. We learn about different use cases as examples from the edge ecosystem.
(ii) DevOps, continuous deployment and micro-services: we present the goals and principles of DevOps. Then we zoom into the subfield of continuous deployment and micro-service based architectures. Finally we end with a hands-on workshop that uses the Teastore micro-service based application and where the students learn to deploy a new version of the application without any downtime.

More specifically, the following topics are covered.

 Copyright © 5GhOSTS Consortium 2019-2023

I. Introduction and use cases
   a. Edge Computing Introduction
   b. The Emerging Edge Landscape
   c. Distributed Cloud Infrastructure and 5G
   d. MELA 5G Webinar: Edge Computing and Distributed Cloud
   e. Business perspective
   f. The Future of Edge Computing, current status and outlook:
   g. Private LTE/5G and Edge Computing:

II. DevOps, micro-services and the deployment pipeline
   a. What is DevOps
   b. Why DevOps?
   c. DevOps-aware software architecture
   d. Micro-services: architectural principles and examples
   e. The deployment Pipeline
   f. The "Teastore" micro services based application

III. Hands-on workshop
   a. a practical game where the ESRs will experience the advantages and disadvantages of DevOps and Microservices. This requires some preparation in advance where each ESR will need to deploy a Kubernetes cluster on the Ericsson cloud and deploy a particular version of Teastore on that cluster.

In M26, the second part of the training will be conducted. Its curriculum consists of the following two parts:

(i) Cloud architecture and security: We learn about the basics of SDN and NFV. Common SW components from the edge cloud SW stack are explored in a hands-on training provided by EST. Moreover, we study common cloud, IoT, and network security issues. We discuss current trends and open issues in the edge cloud architecture with an expert from Ericsson Research
(ii) Standardization and 5G integration: we give an overview of the 5G architecture as well as the ETSI MEC and 5G edge computing standards. We discuss the current state of integration in standardization work with an Ericsson 3GPP SA2 expert.

3.4 Intellectual Property Rights (IPR) training

The goal of the training is to introduce the students to the protection of their ideas by means of writing down their ideas in the form of Invention Disclosure (IvDs). IvDs are developed into patent applications and submitted to a patent office if internally at Ericsson an IvD is decided to be filed as a provisional or full patent application. The patent application process is a lengthy process which can take more time that the span of the 5GhoSTS project. However it is important that the students learn how to participate in intellectual property protection first steps until the filing of the patent application to a patent office. The specific goals of this training is for the students to learn how to

(i) Search for prior art, i.e. existing patent applications that may solve the problem that they are trying to solve, using special tools
(ii) Read existing patent applications
(iii) Write invention disclosures that are pre-patent documentation of the idea
(iv) Assist the patent engineers and patent lawyers in drafting the patent application

Copyright © 5GhOSTS Consortium 2019-2023

The training consists of the following modules

I. Patent Basics - An introduction to Patents at Ericsson, Ericsson online course describing intellectual property and why it is important.
II. Patent Basics - From Idea to Patent, Ericsson online course focusing on the Invention Disclosure writing and searching for prior art (related work).
III. From Idea to Patent, recorded seminar of one of Ericsson's Experts participating in the regular patent boards to give practical advice about producing patents.
IV. Apart from these basic courses, a recorded seminar about creativity could also be offered to the students later on when they have a first exposure to patent reading and writing the IPR protection.
V. In addition Ericsson has offered a hands on workshop with the following agenda
    a. Prerequisite: Before the workshop each ESR had to find one idea to develop as an IvD. The "Idea generation" took place a group meeting following a forced association methodology.

    At the day of the workshop, the following steps are followed.

    b. Introduction to the exercise (5-10 min)
    c. Students receive the IvD template and retreat to their office to write down their idea in the IvD template. In parallel the students perform prior art search and capture this in the Background of the IvD.
    d. Students meet at the end of the half day and present their ideas to a dummy patent board during which they need to answer the questions of the patent board at least with respect to novelty, inventive step and business relevance. If the ideas are actually novel and not made up only for the IvD writing workshop the students may be encouraged to submit the IvD to be considered for a regular patent board.

    The supervisor offers support to the students' question while IvD writing is in session.

VI. Open source training: With respect open source, Ericsson has processes about how to handle open source as input to Ericsson work (e.g. use open source software in a project/product) and how to handle open source as output (any internally developed closed source can be opened). These processes were explained in a meeting with an Ericsson open source expert.

3.5. Industry-oriented conference attendance

The following conferences have been attended by our ESRs:

I. FOSDEM 21: *"FOSDEM is a free event for software developers to meet, share ideas and collaborate. Every year, thousands of developers of free and open source software from all over the world gather at the event in Brussels. In 2021, we gather online"*[9]. ESR1 presented his latest results in the context of KU Leuven's ongoing work on authentic execution for secure-sensitive networked applications. ESR1 and ESR3 have attended this conference.

[9] https://fosdem.org/2021/

 Copyright © 5GhOSTS Consortium 2019-2023

II. OC3 2021: Open Confidential Computing Conference: "*The Open Confidential Computing Conference (OC3) is the online conference for all topics related to Confidential Computing. In a nutshell, Confidential Computing enables the always encrypted and verifiable processing of data on potentially untrusted computer systems - could be your own computer or a machine in the cloud. While this addresses many security and privacy problems and enables exciting new data-driven business models, only few people know how to use Confidential Computing and even fewer have applied it in practice. OC3 aims to help change this*"[10]. Trusted computing is one possible approach to achieve confidential computing. As such this conference is fully in scope of the 5GhOSTS project. ESR1 and ESR3 have attended this conference.

III. KubeCon Europe 2021[11]: This conference gathers adopters and technologists from leading open source and cloud native communities. Latest developments of technologies include reports about Kubernetes, Open Policy Agent, Container Network Interface, KubeEdge, SPIFFE, SPIRE. These technologies are all in scope of the 5GhOSTS project. ESR2 has attended this conference.

4. Local trainings

Local trainings primarily concern trainings on transferrable skills. For trainings on transferrable skills, these trainings are optional and mixed and matched by ESRs as they see fit in function of their own career development plan. These trainings are organized by the aforementioned partners within KU Leuven and Ericsson. As with network-wide trainings, these trainings are also organized in a virtual format and ESRs should register for slots whenever deemed suitable.

4.1 ESR1

Ericsson

Introduction to 5G

Cloud security management

Security fundamentals

OpenStack basics

KU Leuven

Seminar on research integrity

Teaching assistant training

Networking for researchers: The basics

External

Tenth Summer School on Formal Techniques Stanford Research Institute (SRI)

5G: Enabling Technologies, Opportunities and Research Challenges Ahead University of Pisa

Introduction to Standardization by ITN-EID Heart project

[10] https://hopin.com/events/oc3-2021

[11] https://events.linuxfoundation.org/archive/2021/kubecon-cloudnativecon-europe/

Copyright © 5GhOSTS Consortium 2019-2023

4.2 ESR2

Ericsson

- OpenStack basics

KU Leuven

- Brand your career profile
- Introduction to leadership
- ITN complimentary skills training: Basics of IP protection and valorization
- Managing your PhD
- Networking for researchers: The basics
- Open science: Internal course on open Access in H2020
- Open Science Study Day
- Research integrity: Course on Research integrity for starting PhDs
- Introduction to Standardization
- SWEET2 (Starters Week of Engineering and Education: Training for TAs)
- Interuniversity Job Market for Young Researchers

External:

- WIC Midwintermeeting 2021: 5G and Beyond- Technologies for a New Application Era
- Introduction to Standardization by ITN-EID Heart project

4.3 ESR3

Ericsson

- Introduction to 5G
- Cloud security management
- Security fundamentals
- OpenStack basics

KU Leuven

- Academic writing
- Seminar scientific integrity
- Female Brain Power

External

 Copyright © 5GhOSTS Consortium 2019-2023

Academic English: Writing Specialization by Coursera

Tenth Summer School on Formal Techniques Stanford Research Institute (SRI)

Introduction to Standardization by ITN-EID Heart project

4.4 ESR4

Ericsson

Openstack basics

KU Leuven

Privacy Law and Data Protection

Creative problem solving

Brand your career profile

Introduction to leadership

Managing your PhD

Central Lecture Research Integrity

Networking for researchers: the basics

Successful Negotiation: Essential Strategies and Skills

External:

Introduction to Software Product Management

Introduction to the Internet of Things and

Embedded Systems

Intel Network Academy – Network Transformation 101

Software Processes and Agile Practices

Smart Device & Mobile Emerging Technologies

Introduction to Risk Management

IoT (Internet of Things) Wireless & Cloud Computing Emerging Technologies

Intel Network Academy – Network Transformation 102

IT Security: Defense against the digital dark arts

Secure Coding Practices

5G: Enabling Technologies, Opportunities and Research. Challenges Ahead

Bucerius Legal Tech Essentials

Introduction to Standardization by ITN-EID Heart project

Copyright © 5GhOSTS Consortium 2019-2023

 Copyright © 5GhOSTS Consortium 2019-2023