Supplementary Module of School of Engineering

Title: Future Networks and Security

Short Code: EVA_FutNWSec

Number of credits	3 ECTS
Organizer	InIT Institute of Applied Information Technology
Performance record	Presentations (20 minutes, final one typically within the Information Security Research Group (ISE) at InIT) and a term paper (6 pages, 2-column IEEE conference format). This review paper reports on the problem investigation, related work and its analysis (e.g., weaknesses and strengths), proposed designs and/or contributions in those works, and conclusion.
Start date	First week of fall and spring semesters, by arrangement
Language	English
Abstract (max. 300 characters)	The course consists of an introductory session and topic assignment to students (selectable by them). Regular colloquia with all participants to discuss findings and a short paper presentation by one of the students per week; and a final where each participant gives a final presentation on his topic based on their final paper.
Module content and learning objectives	We read and discuss original research publications in the future networks and security domain. Toward this goal, the topics of interest include, but are not limited to: - 5G and 6G security - Machine learning/AI and network security - Blockchain and security - Drone and satellite networks security - Device-centric and IoT security - Secure network softwarization - Service infrastructure security - Multi-access Edge Computing (MEC) security - Trusted computing The learning goals of this course are as follows: - You learn about a specific topic in the network security context. - You have an understanding of technical challenges, solutions and potential research directions regarding future networks and security. - You can identify relevant research work in the literature, read their outcomes (i.e., technical papers), assess and analyze them with critical thinking - You can communicate your findings and your deduced knowledge in a concise and clear form as talks and written papers

Supplementary Module of School of Engineering

Preconditions	The module is intended for students with a background in computer networks and information security. Therefore, students should have knowledge of basic IT security topics such as cryptography and network security. Moreover, a good knowledge of computer networks and protocols are expected.
Literature	An initial set of papers will be provided but you can bring your own based on your technical interests in this domain.
Specific regulations	
Contact and information	Dr. Gürkan Gür, gurkan.gur@zhaw.ch