Syllabus
Advanced topics within Cybersecurity, 6hp

Issued by the WASP graduate school management group

Main field of study
Autonomous Systems, Software

Course level
PhD student course

- AS track: elective
- SO track: elective
- AI track: elective
- Joint curriculum: Advanced

Course offered for
PhD students in the WASP graduate school. The examiner is Prof. Andrei Gurtov (LiU).

Entry requirements
This is an advanced course targeting students with good knowledge in information security, network protocols TCP/IP and mathematics (e.g., modular arithmetics) and basic cryptography. Prior knowledge of cryptography (hash functions, symmetric and asymmetric crypto, digital signatures) is required. Network competence should cover IPSec, TLS, basic intrusion detection and firewall skills. Participants should have basic familiarity with probability and programming. Prior background in basics of data privacy is assumed.

Intended learning outcomes
For a passing grade the student must

- be able to describe some of the main primitives used in post-quantum cryptography
- show familiarity with some of the main primitives used in secure multi-party computation
- be able to describe how fully homomorphic encryption works and describe some main variations
- Understand and demonstrate use of advanced IPsec modes and key exchange with Internet hosts
- Show competence with Internet secure mobility and multihoming protocols
- Demonstrate the use of data privacy tools

The students shall learn advanced cryptography tools and algorithms and apply those to secure network protocols, such as Host Identity Protocol (HIP) and to achieve data privacy. There is natural flow of the course material, from crypto to network security followed by data privacy at different system levels.

Course content
Module 1: Introduction to practical and modern cryptology

Site: Lund University, Dept. of EIT

Duration: Two days

Teacher: Prof. Thomas Johansson

This module contains post-quantum crypto, secure multi-party computation, and fully homomorphic encryption, some of it with direct relevance to AI/ML. The post-quantum crypto part will introduce LWE and the new standards ML-KEM and ML-DSA. The secure multi-party computation part will introduce how to compute with private data, with concepts like secret sharing, zero-knowledge proofs, oblivious transfer, etc. The last part is devoted to fully homomorphic encryption, i.e., computing on encrypted data, and its applications in AI/ML.

Content: 4h lectures per day, 2 hours of exercise/lab training per day.

Module 2. Secure Mobility and Multihoming with Host Identity Protocol (HIP)

Site: Valla, Linköping University

Duration: Two full days

Teacher: Prof. Andrei Gurtov (help from TAs in AEGIS group at CYBER division).

This module focuses on network and application security. The Host Identity Protocol (HIP) is an IETF-standardized secure networking protocol that separates the dual role of IP addresses (location vs. identification) by introducing a new cryptographic namespace. It enhances network security, supports mobility (maintaining connections while moving), and enables multi-homing by decoupling endpoint identifiers from topological locators, often used in aerospace, defense, and IoT. We study HIP design and architecture, practical use scenarios, and touch upon Post-Quantum Cryptography deployment.

Content: 2-4h lectures per day, 2-4 hours cyberlabs. Labs will include a virtual networking environment to do HIP connections, IPsec tunnels and firewall config.

Recommended textbook: "Host Identity Protocol (HIP): Towards the Secure Mobile Internet" https://www.wiley.com/en-ie/Host+Identity+Protocol+(HIP)%3A+Towards+the+Secure+Mobile+Internet-p-9780470772904

Module 3. Data Privacy

Site: Göteborg, Chalmers University

Duration: Two full days

Teacher: Prof. Alejandro Russo <russo@chalmers.se>.

This module focuses on the theory and practice of data privacy, with Differential Privacy (DP) as its central framework. Data privacy has become a critical concern in modern data systems, yet many classical protection mechanisms — from access control to ad hoc

anonymization — offer weaker guarantees than commonly assumed. This module addresses that gap by building rigorous, mathematically grounded intuitions alongside practical implementation skills.

The lecture component opens with the landscape of privacy failures: why access control is insufficient, how de-identification can be circumvented, and what formal privacy should mean. We then develop the core theory of differential privacy from the ground up — covering the formal definition, pure and approximate variants, and the Laplace mechanisms. A substantial part of the lectures is devoted to the compositional properties of DP (post-processing resilience, sequential and parallel composition, group privacy) and to sensitivity analysis, which bridges the gap between abstract definitions and concrete query design. The final topics of this module address system-level concerns: how to architect a differentially private statistical database, and how to track stability through data transformations. The lab session gives participants hands-on experience implementing core DP mechanisms, exploring the privacy–accuracy tradeoff, and reasoning about budget consumption in a realistic pipeline setting.

Content: 4h lectures per day, 2 hours exercise/labs.

Teaching and working methods

There will be a combination of lectures, exercises and labs in computer rooms.

Examination

Each module contains a collection of labs, programming assignments and hand-in exercises, for which the results and solutions are collected in a homework report in each module. They all need to be approved to get a passing grade.

The assignments will be part of the onsite lab sessions (with a follow-up submission of late tasks). There will be one submission report per each module. Students need to pass all assignments to get a passing grade. Solution code and lab reports are required.

Grades

Pass or fail.