Course syllabus

Avancerad webbsäkerhet
Advanced Web Security

EITN41, 7,5 credits, A (Second Cycle)

Valid for: 2023/24
Faculty: Faculty of Engineering, LTH
Decided by: PLED C/D
Date of Decision: 2023-04-18

General Information

Language of instruction: The course will be given in English

Aim

The course aims at deepen the student's knowledge about the security problems and solutions that relate to web based technology. Some areas requiring use of cryptographic primitives will be addressed in detail. Knowledge of these will give the student tools to understand also related areas.

Learning outcomes

Knowledge and understanding
For a passing grade the student must

- Describe some advanced security problems that arise when using web based services.
- Describe how cryptographic data can be represented on the web.
- Describe possibilities and problems related to e-commerce and electronic payments.

Competences and skills
For a passing grade the student must

- Be able to analyze the security protocols, identify weaknesses and problems and be able to propose solutions.
- Show that you understand the technical solutions that are used to avoid a security flaw.
- Show that you understand the security limitations in the protocols.
- Apply the design choices of the studied protocols to other protocols.

- Be able to implement a given security protocol

Judgement and approach
For a passing grade the student must

- Be able to discuss and present your solutions to the home assignments.
- Be able to discuss the design choices of the security protocols discussed in the course.

Contents

Data representations: CMS, ASN.1, BER, CER and DER encoding

PKI and Web Security: PKCS#12, CRL, OCSP, signing procedures, identity based cryptosystems

Anonymity: Anonymity solutions, Chaum mixes, Tor, attacks

E-voting: E-voting protocols, homomorphic encryption, ZK-proofs, threshold decryption

Secure messaging: OTR, the Signal protocol

e-commerce: Electronic payments, SET, 3D Secure, Bitcoin and Blockchains, untraceable E-cash

All course material and lectures will be in English.

Examination details

Grading scale: TH - (U,3,4,5) - (Fail, Three, Four, Five)
Assessment: Home assignments, which are graded, gives grade 3 or 4. If grade 4 is achieved on home assignments, grade 5 can be obtained after successful oral exam.

The examiner, in consultation with Disability Support Services, may deviate from the regular form of examination in order to provide a permanently disabled student with a form of examination equivalent to that of a student without a disability.

Admission

Assumed prior knowledge: EIT060/EITA25 Computer Security, EITF05 Web Security
The number of participants is limited to: No
The course overlaps following course/s: EITN40

Reading list

- Lecture notes.
- Academic articles.

Contact and other information

Course coordinator: Paul Stankovski Wagner, paul.stankovski_wagner@eit.lth.se
Course homepage: http://www.eit.lth.se/course/EITN41
Further information: The course material will be in English.