



LUNDS UNIVERSITET
Lunds Tekniska Högskola

Kursplan för

Avancerad webbsäkerhet Advanced Web Security

EITN41, 7,5 högskolepoäng, A (Avancerad nivå)

Gäller för: Läsåret 2016/17

Beslutad av: Utbildningsnämnd A

Beslutsdatum: 2016-04-05

Allmänna uppgifter

Valfri för: BME5, C4-da, C4-sec, D4-ks, E5

Undervisningsspråk: Kursen ges på svenska

Syfte

Kursen ska ge studenten fördjupad kunskap om de säkerhetsproblem som relaterar till webbt teknologi. En del områden som kräver kryptografiska primitiver kommer behandlas i detalj och en förståelse för dessa ska ge studenten verktyg att applicera sin kunskap på andra säkerhetstekniker.

Mål

Kunskap och förståelse

För godkänd kurs skall studenten

- Beskriva vissa avancerade säkerhetsproblem som uppstår vid användning av webbaserade säkerhetstjänster.
- Beskriva hur kryptografisk data kan representeras på webben.
- Beskriva möjligheter och problem relaterade till e-handel och elektroniska betalningar.

Färdighet och förmåga

För godkänd kurs skall studenten

- Kunna analysera säkerhetsprotokoll, identifiera svagheter och problem, och föreslå lösningar.
- Visa förståelse för de tekniska lösningarna som finns för att undvika säkerhetsproblem.
- Visa förståelse för säkerhetsbegränsningarna i de berörda protokollen.
- Applicera designval i de berörda protokollen på andra protokoll.

Värderingsförmåga och förhållningssätt

För godkänd kurs skall studenten

- Kunna diskutera och presentera lösningarna till hemuppgifter.
- Kunna diskutera designbeslut i de säkerhetsprotokoll som berörs i kursen.

Kursinnehåll

Datarepresentation: CMS, ASN.1, BER, CER och DER-kodning

Säkerhet i webbtjänster: SOAP, REST, SAML, XML Signaturer och kryptering, WS-* standarder, OAuth, OpenID

PKI: CRL, OCSP, RA, CA, och signeringsprocedurer

Anonymitet: Anonymitetslösningar, Chaum-mixar, Tor, attacker

Elektroniska val: protokoll för elektroniska val, homomorfisk kryptering, ZK-proofs, threshold decryption

e-handel: Elektroniska betalningar, SET, 3D Secure, Bitcoin, microbetalningar, untraceable E-cash

Säkerhet i webbserverar: ModSecurity

Allt kursmaterial kommer att vara på engelska.

Kursens examination

Betygsskala: TH

Prestationsbedömning: Betygsatta hemuppgifter ger betyg 3 eller 4. Om betyg 4 uppnås på hemuppgifter kan betyg 5 erhållas genom muntlig tentamen. Godkänd laboration är ett krav för godkänt i kursen.

Antagningsuppgifter

Förutsatta förkunskaper: EIT060 Datasäkerhet, EITF05 Webbsäkerhet

Begränsat antal platser: Nej

Kursen överlappar följande kurser: EITN40

Kurslitteratur

- Föreläsninganteckningar.
- Akademiska artiklar.

Kontaktinfo och övrigt

Kursansvarig: Dr. Martin Hell, martin.hell@eit.lth.se

Hemsida: <http://www.eit.lth.se/kurs/EITN41>

Övrig information: Kursmaterialet kommer att vara på engelska.