



LUNDS UNIVERSITET
Lunds Tekniska Högskola

Kursplan för

Datasäkerhet Computer Security

EIT060, 7,5 högskolepoäng, G1 (Grundnivå)

Gäller för: Läsåret 2015/16

Beslutad av: Utbildningsnämnd A

Beslutsdatum: 2015-04-10

Allmänna uppgifter

Huvudområde: Teknik.

Obligatorisk för: C2, D3

Valfri för: BME4, E4, F4

Undervisningsspråk: Kursen ges på svenska

Syfte

Kursen syftar att ge studenten en god översikt över de relevanta områden inom datasäkerhet samt fördjupade kunskaper inom några av dessa.

Mål

Kunskap och förståelse

För godkänd kurs skall studenten

- Beskriva de generella problemen inom området datasäkerhet
- Klassificera säkerhetsproblem i förhållande till olika discipliner inom datasäkerhet
- Beskriva olika byggstenar inom datasäkerhet

Färdighet och förmåga

För godkänd kurs skall studenten

- göra översiktliga beskrivningar av system som syftar till att öka säkerheten
- visa prov på förmåga att kunna i grova drag analysera ett säkerhetsproblem
- kunna både muntligt och skriftligt kommunicera resultatet av ett projektarbete

Värderingsförmåga och förhållningssätt

För godkänd kurs skall studenten

Under kursen gång ska studenten kunna redogöra för och diskutera lösningar på utförda projekt.

Kursinnehåll

Inledning: Utvecklingen inom informationsteknologin har gjort datasäkerhet till ett av de stora och relevanta områdena när det gäller utveckling av framtida informationsteknologiska system. Nästan dagligen möter man i dagspressen olika aspekter av datasäkerhet. Detta rör sig om allt ifrån exportrestriktioner för kryptering till datavirus och intrång i datasystem. Kursen har som syfte att ge en översikt över relevanta områden inom datasäkerhet, samt att ge fördjupade kunskaper inom något eller några av dessa.

Grunder: Generella datasäkerhetsprinciper och definitioner, identifiering och autenticering, accesskontroll, tillit och evaluering av säkerhet.

Säkerhetsmodeller: Bell-LaPadula, Biba, Clark-Wilson, Chinese wall.

Säkerhetsvärdering: Orange Book, ITSEC, Common Criteria.

Kryptoalgoritmer: Krypteringsmetoder, hashalgoritmer, digital signering och digitala certifikat, X509, samt public-key infrastructure begreppet (PKI).

Säkerhet i Datorsystem: Säkerhet i operativsystem, säkerhet i Unix/Linux, Windows, Java.

Säkerhetsproblem: Malware, attacker, buffer-overflow, mjukvarusäkerhet.

Distribuerade system: Accesskontroll, Kerberos, brandväggar, intrångsdetektering, nyckeldistribution.

Nätverk: Säkerhet i internet samt radionät som GSM/UMTS och WLAN. Säkerhetsprotokoll TLS/SSL, IPSEC.

Säkerhet i databaser: Accesskontroll, informationsläckage och inferens.

Kursen innehåller även två projekt där slutresultatet ska sammanfattas i en teknisk rapport och sedan presenteras under ett seminarie.

Kursens examination

Betygsskala: TH

Prestationsbedömning: För godkänd kurs och betyg 3 krävs godkända laborationer, godkända projekt och godkända hemuppgifter som görs online. Utöver detta kan frivillig skriftlig tentamen ge betyg 4 eller 5.

Delmoment

Kod: 0111. **Benämning:** Tentamen.

Antal högskolepoäng: 3,5. **Betygsskala:** TH. **Prestationsbedömning:** Hemuppgifter som görs online. För betyg 4 eller 5 krävs dessutom skriftlig tentamen.

Kod: 0211. **Benämning:** Laborationer.

Antal högskolepoäng: 2. **Betygsskala:** UG. **Prestationsbedömning:** Genomgången laboration.

Kod: 0311. **Benämning:** Projekt.

Antal högskolepoäng: 2. **Betygsskala:** UG. **Prestationsbedömning:** Projekt rapport plus presentation.

Antagningsuppgifter

Förutsatta förkunskaper: EDA011, EDA016 eller EDA017 Programmeringsteknik.

Begränsat antal platser: Nej

Kurslitteratur

- D. Gollman: Computer security, 3rd ed. ISBN: 9780470741153.

Kontaktinfo och övrigt

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

Hemsida: <http://www.eit.lth.se/kurs/eit060>