LUNDS UNIVERSITET
Lunds Tekniska Högskola

Kursplan för läsåret 2007/2008

SÄKERHET EDA625

Data Security

Antal högskolepoäng: 7,5. **Betygskala:** TH. **Nivå:** G2 (Grundnivå, fördjupad). **Undervisningsspråk:** Kursen ges på svenska. **Obligatorisk för:** IDA3. **Kursansvarig:** Ben Smeets, ben.smeets@it.lth.se, Ingenjörshögskolan i Helsingborg. **Prestationsbedömning:** För att erhålla betyget 3 krävs godkänd skriftlig tentamen samt godkända redovisningar av i kursen ingående laborationer/redovisningar. Högre betyg avgörs via den skriftliga tentamen. **Hemsida:** http://www.hbg.lth.se.

Syfte

Kursens syfte är att göra datateknikingenjören väl förtrogen med de säkerhetsproblem som behöver lösas kring och i datorsystem för att en betryggande kommunikation skall kunna upprättas. I en värld där kommunicerande datorer är geografiskt utspridda är det viktigt att man säkerställer att rätt information når rätt och endast rätt mottagare. Kryptering, autenticering, nyckelhantering och certifikat är exempel på begrepp som klargörs och exemplifieras i kursen.

Mål

Kunskap och förståelse

För godkänd kurs skall studenten

förstå och förklara grundläggande säkerhetsproblem och lösningar som uppstår i samband med dataanvändning och datakommunikation: sekretess, dataintegritet och tillgänglighet.

Färdighet och förmåga

För godkänd kurs skall studenten

- kunna upptäcka och identifiera problemställningar som uppkommer vid datorhantering och kommunikation mellan datorer.
- kunna känna till olika sätt att hantera eller lösa ovan angivna problem.
- kunna föreslå och/eller redovisa lämpliga åtgärder som gängse används för att säkra data vid datahantering och datakommunikation.
- kunna förklara innebörden av praktiska åtgärder som vidtas för att säkra data och datasystem.

Innehåll

- Säkerhet och sårbarhetsanalyser.

- Tillförlitlig drift.
- Vanliga hot mot säkerheten.
- Mänskliga misstag.
- Virus, maskar och trojaner.
- Identitetsverifiering.
- Säkra operativsystem.
- Behörighetskontroll.
- Skyddsbehov vid lagring och kommunikation av information.
- Kryptering och kryptoteori.
- Kryptobaserade kontrollsummor, signaturer.
- Nyckelhantering.
- Nätsäkerhet.
- Standardlösningar för Internet typ SSI, SET.

Litteratur

Gollman, D: Computer Security. John Wiley And Sons Ltd, UK 1998. ISBN: 0-471-97844-2.