



Kursplan för läsåret 2010/2011  
(Genererad 2010-06-28.)

---

## DATASÄKERHET

### Computer Security

EIT060

**Antal högskolepoäng:** 7,5. **Betygsskala:** TH. **Nivå:** G1 (Grundnivå). **Huvudområde:** Teknik. **Undervisningsspråk:** Kursen ges på svenska. **Obligatorisk för:** C2, D3. **Valfri för:** E4, E4ks, F4. **Kursansvarig:** Dr. Martin Hell, martin.hell@eit.lth.se, Inst för elektro- och informationsteknik. **Förutsatta förkunskaper:** Grundläggande Java-kunskaper. **Prestationsbedömning:** Skriftlig tentamen (5 tim). För godkänt betyg krävs även godkända laborationer samt godkänt projekt. **Poängsatta delmoment:** 3. **Hemsida:** <http://www.eit.lth.se/kurs/eit060>.

#### 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

##### *Värderingsförmåga och förhållningssätt*

För godkänd kurs skall studenten

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

#### Innehåll

*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 autentisering, accesskontroll, tillit och evaluering av säkerhet

*Säkerhetsmodeller:* Bell-LaPadula, Biba, Clark-Wilson

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

*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, polyinstantiering

#### **Litteratur**

Gollmann D.: Computer Security. Andra utgåvan (ISBN 0470862939).

#### **Poängsatta delmoment**

**Kod:** 0111. **Benämning:** Tentamen.

**Antal Högskolepoäng:** 3,5. **Betygsskala:** TH. **Prestationsbedömning:** Skriftligt prov.

**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.