LUNDS UNIVERSITET
Lunds Tekniska Högskola

Kursplan för läsåret 2008/2009
(Genererad 2008-07-17.)

DATASÄKERHET EIT060

Computer Security

Antal högskolepoäng: 7,5. **Betygskala:** TH. **Nivå:** G1 (Grundnivå). **Undervisningsspråk:** Kursen ges på svenska. **Obligatorisk för:** C2. **Valfri för:** D3, E3, F3, RH4. **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 godkända hemuppgifter, laborationer samt godkänt projekt. **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,
- förklara principer bakom olika accesskontrollsmekanismer och digitala signaturer

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 autenticering, access kontroll, tillit och evaluering av säkerhet

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

Säkerhet i Datorsystem: Säkerhet i operativsystem, säkerhet i unix, Windows, Java. Trusted computing group: TPM

Säkerhetsproblem: Malware, attacker, buffer-overflow, mjukvarusäkerhet

Distribuerade system: Accesskontrol, Kerberos, brandväggar, intrångsdetektering

Nätverk: Säkerhet i internet samt radionät som GSM/UMTS och WLAN. Säkerhets protocol TLS, SSL, IPSEC. Virtuella nät som VPN och Darknet

Smarta kort: Historik, arkitektur, Javakort, attacker, verifiering

Säkerhet i databaser: Accesskontroll, informationsläckage, polyinstantiering

Skydd av IP: Skydd av program, musik, film och e-böcker, genomgång av kopieringsproblematiken, principer för ett DRM system.

Litteratur

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