LUNDS UNIVERSITET
Lunds Tekniska Högskola

Kursplan för läsåret 2007/2008

DATASÄKERHET EIT060

Computer Security

Antal högskolepoäng: 7,5. **Betygskala:** TH. **Nivå:** G1 (Grundnivå). **Undervisningsspråk:** Kursen ges på svenska. **Obligatorisk för:** C3. **Valfri för:** D3, E3, F3, RH4. **Kursansvarig:** Prof Ben Smeets, ben.smeets@it.lth.se, Inst f informationsteknologi. **Förkunskapskrav:** Vana att kunna programmera i Java. **Prestationsbedömning:** För slutbetyg 3 krävs godkända övningar, laborationer samt godkända projektuppgifter. Slutbetyg 4-5 kan erhållas via skriftlig tentamen. Förstagångstentamen i ordinarie tentamensperiod: Ja Omtentamen i omtentamensperiod: Nej. **Hemsida:** http://www.it.lth.se/courses/computersecurity.

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 säkerhets problem i förhållande till de olika discipliner inom datasäkerhet
- beskriva olika byggstenar inom datasäkerhet,
- förklara principer bakom olika access kontroll och digitala signaturer

Färdighet och förmåga
För godkänd kurs skall studenten

- göra översiktliga beskrivningar av system som syftar att öka säkerheten
- visa prov på förmåga att kunna i grova drag analysera ett säkerhets problem

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

Krypto algoritmer: Krypterings metoder, digital signering och digitala certifikat, X509, samt public-key infrastructure begreppet (PKI), märkning, kod obfuskering

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

Säkerhetsproblem: Malware, attacker, buffer-overflow, mjukvara säkerhet

Distribuerade system: Access kontrol, 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, Java kort, attacker, verifiering

Säkerhet i databaser: Access kontroll, informationsläckage, polyinstantiering

Skydd av IP: Skydd av program, musik, film och e-böcker, genomgång av kopieringsproblematiken, principer för ett DRM system, Apple Fair Play, OMA DRM v1 och v2.

Litteratur

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