LUNDS UNIVERSITET
Lunds Tekniska Högskola

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

SÄKRA SYSTEM OCH APPLIKATIONER EIT015

Secure Systems and Applications

Antal högskolepoäng: 7,5. **Betygskala:** TH. **Nivå:** G2 (Grundnivå, fördjupad). **Undervisningsspråk:** Kursen kan komma att ges på engelska. **Valfri för:** C4, C4ks, C4sd, D4, D4ks, E4. **Kursansvarig:** Prof Ben Smeets, ben.smeets@eit.lth.se, Inst för elektro- och informationsteknik. **Förutsatta förkunskaper:** EIT060 Datasäkerhet (7,5p) eller EDI051 Kryptoteknik (7,5p). **Prestationsbedömning:** För slutbetyg 3 eller 4 krävs godkända projektuppgifter som blir betygsatta. Slutbetyg 5 kan erhållas via skriftlig eller muntlig tentamen. Studenterna måste anmälla sig alltid till skriftlig eller muntlig tentamen. **Hemsida:** http://www.eit.lth.se/kurs/eit015.

Syfte

Kursen syftar att ge studenten en fördjupad insikt i vissa problem och lösningar inom datasäkerhet för att kunna på egenhand välja rätt bland existerande lösningar samt att kunna komma med kvalitativt goda lösningsförslag.

Mål

Kunskap och förståelse
För godkänd kurs skall studenten

- Analysera ett säkerhets problem i ett datorsystem
- Komma med kvalitativt goda föreslag till lösningar för många standard datasäkerhets problem
- Redogöra för olika byggstenar inom datasäkerhet
- Förstå mekanismer bakom de mest använda attack metoder

Färdighet och förmåga
För godkänd kurs skall studenten

- göra ingående beskrivningar av system som syftar att öka säkerheten
- motivera lösnings förslag till ett säkerhets problem

Värderingsförmåga och förhållningssätt
För godkänd kurs skall studenten

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

Innehåll
Inledning: Att kunna bygga säkra informationssystem och (dator) applikationer kräver ingående kunskaper inom datorsäkerhet. Speciellt, är det viktigt att förstå hur olika säkerhets protokoll och kryptografiska metoder tillämpas för att skapa säkra applikationer. Eftersom system kommer att bli attackerad så är det också viktigt att förstå hur man ska analysera attackerade system på ett professionellt. Samtidigt måste man förstå hur den lede fi arbetar för att få sitt mål.

Computer Forensics: principer, tillvägagångssätt

Digitala signaturer: Digitala signaturer på riktig, Public Key Infrastructure (PKI) (certifikat, revokering, CA, RA, X509), XML signaturer

Speciala krypto algoritmer: blinda signaturer, e-röstning, duala signaturer

E-commerce: solutions (Amazon.com, SET, E-cash), micro-betalning,

DRM system: DRM (ebook, OMA DRM Phase 2),

Smarta kort: ISO standard, programmering

Säkra nätverk: autenticeringsmetoder, RADIUS, DIAMETER, beskrivning och jämförelse av IPSEC/VPN, TLS, SSL. WLAN. UMTS, Denial of Service (DOS) attacker, Internet security,

Litteratur
Föreläsningsanteckningar i form av Powerpoint slides samt artiklar.