



LUNDS UNIVERSITET  
Lunds Tekniska Högskola

*Kursplan för*

## **Avancerad datasäkerhet Advanced Computer Security**

**EITN50, 7,5 högskolepoäng, A (Avancerad nivå)**

**Gäller för:** Läsåret 2012/13

**Beslutad av:** Utbildningsnämnd 1

**Beslutsdatum:** 2012-03-19

### **Allmänna uppgifter**

**Valfri för:** C4, C4-ks, C4-da, D4, D4-ks, E4, E4-ks

**Undervisningsspråk:** Kursen kan komma att ges på engelska

### **Syfte**

Kursen syftar att ge studenten en fördjupad insikt i de huvud problem och lösningar inom datasäkerhet, inbyggda system samt data nätverk. Kursen fördjupar kunskaper av tidigare kurser och ger en analytisk insikt i dagen säkerhetslösningar. Kursen gör det möjligt att 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 eller konsument produkt
- Komma med kvalitativt goda föreslag till lösningar för många standard datasäkerhets och nätverkssäkerhets problem
- Grundinsikt i procedurer för forensic data och nätverksanalys.
- Redogöra för olika byggstenar inom data- och nätverkssäkerhet
- 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 i dator- och nätverksystem
- att kunna genomföra en enkel forensic data- och nätverksanalys procedur

- att kunna analysera och förklara hur existernade skyddsmekanismer fungerar
- att kunna motivera lösnings förslag till ett säkerhets problem

### *Värderingsförmåga och förhållningssätt*

För godkänd kurs skall studenten

Du kommer att tillämpa dina kunskaper i ett antal projekt där du själv (i grupp) ska inhämta ytterligare kunskap in insikter för att slutföra projekten. Kvalitén i motiveringen för lösningar och reflektion över alternativ kommer att bedömas. Inläring av fakta kunskap kommer att understödjas med stöduppgifter som följer kursen.

## **Kursinnehåll**

*Inledning: Att kunna bygga säkra datorsystem, inbyggda system, säkra nätverk, samt (dator) applikationer kräver ingående kunskaper inom datorsäkerhet. Moderna system kommer att arbeta mer autonom och deras säkerhet kommer i allt högre utsträckning bero på tillgängligheten av säkra exekveringsmiljöer. Eftersom system kommer att bli attackerad så är det också viktigt att förstå hur man ska analysera attackerade system på ett professionellt sätt. Kursens innehåll fokuseras på områden; Computer Forensics, Nätverk säkerhet, Plattform säkerhet, DRM och Säker mjukvara.*

### *Computer Forensics:*

- principer
- tillvägagångssätt
- stegeografi
- vertyg

### *Nätverk Säkerhet (huvudområde I):*

- Authentication: Radius och Diameter, Login protokoll,
- Protocoll: DTLS, Säkerhet i mobila nätverk UMTS och LTE, IPSec, typer av VPN lösningar,
- Hot: hot i nätverk, DDOS, Botnets

### *Plattform säkerhet (huvudområde II):*

- Säker exekvering: Speciella operativ system, SELinux, Virtualisering och säkerhet, Java typ VMs,
- Speciella säkerhets hardvara: TCG (TPM), ARM Trustzone, RFID, Smartakort.
- Säkerhet i mobila telefoner: Android, iOS, MeeGo

### *DRM:*

- Basic protection problem,
- Historical perspective on (failed) solutions
- Content protection, SW protection, Licensing systems,
- Obfuscation, white-box cryptography

### *Säker mjukvara (huvudområde III):*

- Vanliga (säkerhets) fel i program,
- Processer för utveckling av säker kod,

- Hjälpverktyg för säker kod utveckling,
- Malware:historik, phishing, clickfraud

#### *Projekt:*

- Project A: Forensic Analys av disc och USB minnes avbilning
- Project B: Samanställning och analys av information från dator och nätverk, proxy och anonymitet
- Project C: DDos attack lab
- Project D: IPSec lab, konfigurerering och trafik loggning
- Project E: Utveckling av säker kod

## **Kursens examination**

**Betygsskala:** TH

**Prestationsbedömning:** För slutbetyg 3 eller 4 krävs godkända projektuppgifter som blir betygsatta. Slutbetyg 5 kan erhållas via muntlig tentamen som täcker projekt och kursmaterial eller godkända test (5st). Studenterna måste alltid anmäla sig till muntlig tentamen. Omtentamen i ordinarie omtentamensperiod: NEJ

## **Antagningsuppgifter**

**Förutsatta förkunskaper:** EIT060 Datasäkerhet (7,5p) eller EDI051 Kryptoteknik (7,5p).

**Begränsat antal platser:** Nej

**Kursen kan ställas in:** Om färre än 8 anmälda.

**Kursen överlappar följande kurser:** EIT015

## **Kurslitteratur**

- Föreläsninganteckningar i form av Powerpointbilder samt artiklar.

## **Kontaktinfo och övrigt**

**Kursansvarig:** Professor Ben Smeets, ben.smeets@eit.lth.se

**Hemsida:** <http://www.eit.lth.se/kurs/eit015>

**Övrig information:** Vid färre än 16 deltagare kan kursen komma att ges med reducerad undervisning och större inslag av självstudier.