



LUNDS UNIVERSITET
Lunds Tekniska Högskola

Kursplan för

Avancerad datasäkerhet Advanced Computer Security

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

Gäller för: Läsåret 2015/16

Beslutad av: Utbildningsnämnd A

Beslutsdatum: 2015-04-10

Allmänna uppgifter

Valfri för: C4-da, C4-sec, D4-ks, D4-se, E4

Undervisningsspråk: Kursen ges på engelska

Syfte

Kursen syftar till att ge studenten en fördjupad insikt i huvudproblem och lösningar inom datasäkerhet, inbyggda system samt datanätverk. Kursen fördjupar kunskaper av tidigare kurser och ger en analytisk insikt i dagens säkerhetslösningar. Kursen gör det möjligt att på egen hand välja rätt bland existerande lösningar samt att kunna komma med kvalitativt goda lösningsförslag.

Mål

Kunskap och förståelse

För godkänd kurs skall studenten

- analysera ett säkerhetsproblem i ett datorsystem eller i en konsumentprodukt
- komma med kvalitativt goda förslag till lösningar för många vanliga datasäkerhets- och nätverkssäkerhetsproblem
- ha grundinsikt i procedurer för dataforensik och nätverksanalys.
- redogöra för olika byggstenar inom data- och nätverkssäkerhet
- förstå mekanismer bakom de mest använda attackmetoderna

Färdighet och förmåga

För godkänd kurs skall studenten

- göra ingående beskrivningar av system som syftar till att öka säkerheten i dator- och nätverkssystem
- kunna genomföra en enkel dataforensik- och nätverksanalysprocedur

- kunna analysera och förklara hur existerande skyddsmekanismer fungerar
- kunna motivera lösningsförslag till ett säkerhetsproblem

Värderingsförmåga och förhållningssätt

För godkänd kurs skall studenten

tillämpa sina kunskaper i ett antal projekt där vederbörande själv (i grupp) ska inhämta ytterligare kunskap och insikter för att slutföra projekten. Kvaliteten i motiveringen för lösningar och reflektion över alternativ kommer att bedömas. Inläring av faktakunskap 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 autonomt och deras säkerhet kommer i allt högre utsträckning bero på tillgängligheten av säkra exekveringsmiljöer. Eftersom system kommer att bli attackerade så är det också viktigt att förstå hur man ska analysera attackerade system på ett professionellt sätt. Kursens innehåll fokuseras på två huvudområden: *Plattformssäkerhet* och *Säker mjukvara*.

Kursen kommer också ha fördjupning kring nätverkssäkerhet och korta introduktioner till områden som *dataforensik* och *DRM-skydd*.

Dataforensik (översikt 1)

- Principer
- Tillvägagångssätt
- Steganografi
- Verktyg

Nätverksäkerhet (några fördjupningar):

- Autentisering: Radius och Diameter, Login-protokoll, LTE
- Protokoll: IPSec, typer av VPN-lösningar,
- Hot: hot i nätverk, DDOS, Botnets

Plattformssäkerhet (huvudområde I):

- Säker exekvering: Speciella operativsystem, SELinux, Virtualisering och säkerhet, Java typ VMs,
- Trusted Computing Group: TCG (TPM),
- ARM Trustzone,
- Intel SGX,
- Smarta kort, RFID.
- Säkerhet i mobiltelefoner: Android, iOS

DRM (översikt 2):

- Grundläggande problem,
- Historiskt perspektiv på (misslyckade) lösningar,
- Skydd av innehåll, skydd för mjukvara, Licenssystem,
- Obfuskering, white-box-kryptografi.

Säker mjukvara (huvudområde II):

- Vanliga (säkerhets)fel i program,
- Processer för utveckling av säker kod,
- Hjälperverktyg för säker kodutveckling,
- Skadlig kod: historik, phishing, clickfraud.

Projekt (föreslagna tema)

- Projekt A: Forensikanalys av disk och USB-minnesavbildning
- Projekt B: IPSec, konfigurerings och trafikloggning
- Projekt C: DDoS-attack
- Projekt D: TPM-användning
- Projekt E: Reverse Engineering av binärkod

Kursens examination

Betygsskala: TH

Prestationsbedömning: För slutbetyg krävs godkända projektuppgifter samt godkända tematest (5 st). Slutbetyg 3,4, eller 5 baseras på den sammanlagda individuella tematestprestationen. För betyg 5 kan ytterliga muntliga stickprov förekomma. Slutbetyg kan också fås genom muntlig tentamen men då kan högst slutbetyg 3 eller 4 erhållas. Studenterna måste alltid anmäla sig till muntlig tentamen.

Antagningsuppgifter

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

Begränsat antal platser: Nej

Kursen överlappar följande kurser: EIT015

Kurslitteratur

- Powerpointbilder samt anteckningar kring huvudområden artiklar.

Kontaktinfo och övrigt

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

Hemsida: <http://www.eit.lth.se/kurs/eitn50>

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