LUNDS UNIVERSITET
Lunds Tekniska Högskola

Kursplan för

Avancerad datasäkerhet
Advanced Computer Security

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

Gäller för: Läsåret 2014/15
Beslutad av: Utbildningsnämnd A
Beslutsdatum: 2014-04-07

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 forensic data 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 nätverksystem
- Kunna genomföra en enkel forensic data- och nätverksanalysprocedur

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

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 och insikter för att slutföra projekten. Kvalitén i motiveringen för lösningar och reflektion över alternativ kommer att bedömas. Inlärning 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 följande områden: Computer Forensics, Nätverk säkerhet, Plattformssäkerhet, DRM och Säker mjukvara.

Computer Forensics:

- Principer
- Tillvägagångssätt
- Steganografi
- Verktyg

Nätverksäkerhet (huvudområde I):

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

Platformssäkerhet (huvudområde II):

- Säker exekvering: Speciella operativsystem, SELinux, Virtualisering och säkerhet, Java typ VMs,
- Särskild hårdvara för säkerhet: TCG (TPM), ARM Trustzone, RFID, Smarta kort.
- Säkerhet i mobiltelefoner: Android, iOS

DRM:

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

Säker mjukvara (huvudområde III):

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

- Hjälpverktyg för säker kodutveckling,
- Skadlig kod: historik, phising, clickfraud.

Projekt (föreslagna tema)

- Projekt A: Forensic-analys av disk och USB-minnesavbildning
- Projekt B: Säkerhetsevaluering av lösningar för ”mobile off-loading”
- Projekt C: DDoS-attack
- Projekt D: IPSec, konfigurering och trafikloggning
- 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. 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 överlappar följande kurser: EIT015

Kurslitteratur

- Föreläsningsanteckningar 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/eitn50
Övrig information: Vid färre än 16 deltagare kan kursen komma att ges med reducerad undervisning och större inslag av självstudier.