IL1333 Hårdvarusäkerhet 7,5 hp

Hardware Security

Fastställande

Skolchef vid EECS-skolan har 2019-10-15 beslutat att fastställa denna kursplan att gälla från och med VT 2020 (diarienummer J-2019-2283).

Betygsskala

A, B, C, D, E, FX, F

Utbildningsnivå

Grundnivå

Huvudområden

Teknik

Särskild behörighet

Slutförd kurs i digital design motsvarande IE1204/IE1205.

Undervisningsspråk

Undervisningsspråk anges i kurstillfällesinformationen i kurs- och programkatalogen.

Lärandemål

Efter godkänd kurs ska studenten kunna

- beskriva state-of-the-art hårdvarusäkerhetstekniker och motivera deras tillämpningar och begränsningar
- beskriva hur säkerheten garanteras i en exemplifierande tillämpning
- beskriva hoten mot ett system från hårdvaruperspektiv samt tillgängliga motåtgärder och tillämpa kunskaperna för att välja en lämplig uppsättning av motåtgärder för en viss hotbild.
- analysera och gör en kritisk avvägning mellan systemets prestanda, kostnad och säkerhet samt exemplifiera kompromisser som är tillgängliga för konstruktörer av elektroniska och inbyggda system
- förklara behovet av hårdvarusäkerhetsprimitiver och motivera för- och nackdelar med olika primitiver samt välja en lämplig primitiv för en specifik tillämpning
- använda kunskaperna till att bygga ett litet elektroniskt eller inbyggt system för ökad säkerhet och förklara hur säkerheten garanteras i systemet.

Kursinnehåll

- Fysiska attacker och "tamper resistance"
- Sidokanalattacker och motåtgärder
- Introduktion till lightweight cryptography
- Säkerhet för smartkort och radiofrekvensidentifiering (RFID-taggar)
- Design för fysikaliska okloningsbara funktioner (PUFs) och sanna slumptalsgeneratorer
- Personlig integritet i sakernasinternet-eran

Examination

- LABA - Laborationer, 2,5 hp, betygsskala: P, F
- PROA - Projekt, 1,0 hp, betygsskala: P, F
- TENA - Skriftlig tentamen, 4,0 hp, betygsskala: A, B, C, D, E, FX, F

Examinator beslutar, baserat på rekommendation från KTH:s handläggare av stöd till studenter med funktionsnedsättning, om eventuell anpassad examination för studenter med dokumenterad, varaktig funktionsnedsättning.

Examinator får medge annan examinationsform vid omexamination av enstaka studenter.

När kurs inte längre ges har student möjlighet att examineras under ytterligare två läsår.

Övergångsbestämmelser

Studenter som har kvar tidigare moment erbjuds att slutföra dessa.

Etiskt förhållningssätt

- Vid grupparbete har alla i gruppen ansvar för gruppens arbete.
- Vid examination ska varje student ärligt redovisa hjälp som erhållits och källor som använts.
- Vid muntlig examination ska varje student kunna redogöra för hela uppgiften och hela lösningen.