FIL3030 Hårdvarusäkerhet 7,5 hp

Hardware Security

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

Fastställande

Kursplan för FIL3030 gäller från och med VT19

Betygsskala

P, F

Utbildningsnivå

Forskarnivå

Särskild behörighet

Antagen som doktorand.

Undervisningsspråk

Undervisningsspråk anges i kurstillfällesinformationen i kurs- och programkatalogen.

Lärandemål

Syftet med kursen är att ge doktorander kunskap som krävs för att utveckla säkra system. I en tid präglad av sakernas internet där fysiska enheter såsom sensorer och RFID-tags är integrerade med elektronik för att kunna detektera, beräkna och kommunicera blir det en stor utmaning att garantera systemens säkerhet. För att ta itu med detta problem gör

industrin ansträngningar på flera nivåer såsom kryptografiska algoritmer, protokoll, säkra integrerade kretsar, hårdvara arkitektur. Från den akademiska sidan, finns ett ansvar att utbilda och förbereda studenterna - framtidens ingenjörer, för säkerhetsutmaningar i sakernas internet eran. I den här kursen, strävar vi speciellt efter att göra eleverna medvetna om potentiella hårdvarusårbarhet och att erbjuda nödvändiga kunskaper och färdigheter för att bygga pålitlig hårdvara.

Efter avslutad kurs kommer eleverna att kunna:

- Beskriva state-of-the-art hårdvarusäkerhets-tekniker och motivera deras tillämpningar och begränsningar. Beskriva hur säkerheten garanteras i en exemplifierande tillämpning.
- Beskriva hoten mot ett system från hårdvaruperspektiv samt tillgängliga motåtgärder. Tillämpa kunskaperna för att välja en lämplig uppsättning av motåtgärder för en viss hotbild.
- Analysera och göra en kritisk avvägning mellan systemets prestanda, kostnad och säkerhet. Exemplifiera vissa av de kompromisser som är tillgängliga för konstruktörer av elektroniska och inbyggda system.
- Förklara behovet av hårdvaru säkerhets-primitiver. Motivera för- och nackdelar med olika primitiver och välj en lämplig primitiv för en specifik tillämpning.
- Använda kunskapen till att bygga ett litet elektroniskt eller inbyggt system för ökad säkerhet i ett gruppprojekt. Förklara hur säkerheten garanteras i systemet.

Kursinnehåll

Följande är en lista över ämnen som kommer att behandlas:

- Fysiska attacker och "tamper resisance".
- Sidokanalattacker och motåtgärder.
- Introduktion till lightweight cryptography.
- Säkerhet av smartkort och radiofrekvensidentifiering (RFID) taggar.
- Design för fysikaliska unclonable funktioner (PUFs) och sanna slumptalsgeneratorer.
- Personlig integritet i sakernas internet eran.

Kursupplägg

Kursen består av 12 2-timmars föreläsningar, två 4-timmars labs och ett gruppprojekt.

Kurslitteratur

M. Tehranipoor and C. Wang. Introduction to Hardware Security and Trust. Springer, 2012.

Utrustning

Inga

Examination

- EXA1 - Examination, 7,5 hp, betygsskala: P, 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.

I examinationsdelen ingår följande:

- två laborationer (20%, betygsskala godkänd/underkänd), 1.5 hp
- en tentamen (40%, betygsskala A, B, C, D, E, FX, F), 3 hp
- ett forskningsprojekt och dess presentation (40%, betygsskala godkänd/underkänd), 3 hp

Övriga krav för slutbetyg

För att bli godkänd bör alla punkter som anges i examinationsmomentet slutföras.

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.