IV1013 Introduktion till datasäkerhet 7,5 hp

Introduction to Computer Security

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

Fastställande

Kursplan för IV1013 gäller från och med VT17

Betygsskala

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

Utbildningsnivå

Grundnivå

Huvudområden

Teknik

Särskild behörighet

- IK1203 Nätverk och kommunikation eller motsvarande.
- IX1500 Diskret matematik eller motsvarande.
- ID2206 Operativsystem eller motsvarande.

Undervisningsspråk

Undervisningsspråk anges i kurstillfällesinformationen i kurs- och programkatalogen.

Lärandemål

Kursen ger en introduktion till grunderna inom kryptografi, säkerhet inom datorsystem och nätverkssäkerhet. Det innebär att efter fullgjord kurs ska studenten kunna

- förklara grundläggande mekanismer i och uppbyggnaden av säkra kommunikationsprotokoll
- beskriva svagheter i datorsystem, mjukvara, nätverk och kommunikationsprotokoll samt förklara attacker som utnyttjar svagheterna
- förklara och jämföra för- och nackdelar med vanliga kryptografiska tekniker
- designa och implementera enklare kryptografiska tillämpningar
- redogöra för och känna igen hot mot informationssäkerhet: konfidentialitet, integritet och tillgänglighet. samt välja lämpliga metoder för att skydda sig mot hot
- designa, implementera och utvärdera säkerhet i nätverk.

Kursinnehåll

- Grundläggande kryptografi: symmetrisk och assymetrisk kryptografi.
- Kryptografisk hashning och digitala signaturer.
- Säkerhet i Internets protokoll och tjänster.
- Certifikat och infrastrukturer för öppen nyckel-kryptering.
- Säkerhet i nätverkssystem: routrar, brandväggar och system för att detektera intrång.
- Säkerhet i operativsystem.
- Mjukvarusäkerhet: sårbarhet, attacker och skyddsmekanismer.

Kurslitteratur

Goodrich, Tamassia: Introduction to Computer Security: Pearson New International Edition - Se vidare: http://catalogue.pearsoned.co.uk/educator/product/Introduction-to-Computer-Security-Pearson-New-International-Edition/9781292025407.page#sthash.aaLrqfj7.dpuf

Examination

- INLB - Inlämningsuppgift, 1,5 hp, betygsskala: P, F
- PRO1 - Projektuppgift, 6,0 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.

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.