IK2206 Säkerhet och datasekretess på internet 7,5 hp

Internet Security and Privacy

Fastställande

Betygsskala

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

Utbildningsnivå

Avancerad nivå

Huvudområden

Datalogi och datateknik, Elektroteknik

Särskild behörighet

Kunskaper i datornätverk, 6 hp, motsvarande slutförd kurs EP1100/IK1203/IK2218/EP2120.

Färdigheter i engelska motsvarande gymnasiekursen Engelska B/6.

Lärandemål

Efter godkänd kurs ska studenten kunna

- förklara principerna bakom kryptering med delade nycklar
- motivera designprinciperna för blockchiffer
- välja lämpliga användningsmetoder för blockchiffer
- förklara principerna för hashning av meddelanden
- använda meddelandekoder för integritetsskydd
- förklara principerna för asymmetrisk kryptering
- välja lämpliga autentiseringsmetoder
- förklara designen av standardiserade tekniker för säker kommunikation som till exempel Kerberos, IPsec, SSL/TLS och PKI
- redogöra för hot mot och svagheter hos vanliga internettillämpningar som e-post och webben
- designa, implementera och utvärdera en säker tillämpning enligt klient-servermodellen

i syfte att få fördjupad kunskap om de tekniker som används för att skapa säkra kommunikationsprotokoll.

Kursinnehåll

- Grundläggande kryptografi och informationsteori: substitutions-, mono- och polyalfabetiska chiffer, homofoniska chiffer och transpositionschiffer.
- Blockchiffer: egenskaper hos och implementering av blockchiffer samt deras användning.
- Asymmetrisk kryptering: RSA, Diffie-Hellman. Egenskaper och användning.
- Hashalgoritmer och digitala signaturer. Egenskaper hos meddelandehashning samt hur integritet och autenticitet kan säkerställas.
- Publika nyckelsystem och certifikat.
- Autentisering av användare: lösenord, biometriska metoder och multifaktorautentisering.
- Autentiseringsprotokoll för etablering av privat och integritetsskyddad kommunikation, principer och egenskaper. Grunderna i Kerberos.
- Nätverkssäkerhet, brandväggar och virtuella privata nät. IPsec.
- Webbsäkerhet: attacker, nätfiske och webbkodinjektion. Säker webbkommunikation med SSL/TLS.
- E-postsäkerhet: attacker och oönskad e-post. Metoder för säker e-post, S/MIME och PGP.
- Design och implementering av säkra tillämpningar med stöd för autentiserad, integritetsskyddad och konfidentiell kommunikation med hjälp av Javas applikationsprogrammeringsgränssnitt.

Examination

- PROA - Projekt, 1,5 hp, betygsskala: P, F
- UPGA - Uppgift, 1,5 hp, betygsskala: P, F

• TENA - Tentamen, 4,5 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.

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.