Försättsblad till skriftlig tentamen vid Linköpings universitet

Datum för tentamen	2016-02-25
Sal (1)	TER3
Tid	8-12
Kurskod	TDDD82
Provkod	TEN1
Kursnamn/benämning **Provnamn/benämning**	Projekttermin inklusive kandidatprojekt: Säkra, mobila system Informationssäkerhet: Skriftlig tentamen
Institution	IDA
Antal uppgifter som ingår i tentamen	9
Jour/Kursansvarig Ange vem som besöker salen	Marcus Bendtsen
Telefon under skrivtiden	0733-140708
Besöker salen ca klockan	09:00 samt 11:00
Kursadministratör/kontaktperson (namn + tfnr + mailaddress)	Madeleine Häger Dahlqvist 282360 madha@ida.liu.se
Tillåtna hjälpmedel	Inga
Övrigt	
Antal exemplar i påsen	

Skriftlig tentamen

TDDD82 Projekttermin inklusive kandidatprojekt: Säkra, mobila system

2016-02-25

Tillåtna hjälpmedel
Inga

Jourhavande lärare
Marcus Bendtsen

Betyg
Ditt betyg på säkerhetsdelen av kursen avgörs av hur många poäng du får på tentamen. Nedanstående betygsgränser är preliminära.

Betyg	3	4	5
Poäng	33	40	46

Instruktioner
För varje fråga står det i fetstil hur många poäng frågan är värd. För varje deluppgift står det sedan hur många poäng man maximalt kan få för deluppgiften. Se exemplet nedan (exemplet ingår inte i tentamen). Totalt ger uppgiften 4 poäng, och man kan svara på de två första deluppgifterna för att få 2 av dessa 4 poäng.

Fråga 0: Historia (4p)

(a) I vilket land föddes Alan Turing? (1p)

(b) Var Alan Turing aktiv vid Bletchley Park? (1p)

(c) Förklara vad man menar med en *Turing Machine*. (2p)

Fråga 1: Säkerhetsbegrepp, policy och mekanism (5p)

(a) Vad är en säkerhetspolicy? (1p)

(b) Vad innebär det att en säkerhetsmekanism är säker? (1p)

(c) Förklara hur vi kan öka tilliten till en mekanism. (3p)

Fråga 2: Kryptoteknik (10p)

(a) Rita två diagram, ett som visar hur ECB mode fungerar och ett som visar hur CBC mode fungerar. Ge en kort förklaring till diagrammen. (2p)

(b) Rita och förklara detaljerna för hur ett Feistelnätverk används i DES (detaljerna för hur funktionen F ser ut och fungerar skall inte ingå). (4p)

(c) Givet de publika nycklarna e och n i RSA, hur krypterar man ett meddelande? (2p)

(d) Hur skapas de publika nycklarna i Diffie-Hellman? (2p)

Fråga 3: Accesskontroll (4p)

Antag att mängden objekt är $O = \{p, q, t\}$, att mängden subjekt är $S = \{a, b, c\}$ och att mängden rättigheter är $R = \{r, w, x\}$. Låt $x(a, p)$ betyda att a har rättighet x på p.

Skapa en accesskontrollmatris och en *capability list* för detta system så att följande policy uppfylls: (4p)

- $\forall s \in S : x(s, p)$
- $w(a, p)$, $w(a, q)$, $w(c, p)$
- $r(b, q)$, $r(c, t)$
- Om inget annat anges så ges inga rättigheter.

Fråga 4: Policymodeller (5p)

Förklara Biba integrity model när *strict integrity policy* används. Förklara med ett exempel så att det är tydligt vilka koncept som ingår och vilka funktioner som används. Det skall bland annat vara tydligt vilka regler som gäller för läsning och skrivning och hur dessa regler är definierade. (5p)

Fråga 5: Hash-funktioner (6p)

(a) Antag att A och B har en hemlig nyckel k. Redogör för hur A och B kan garantera att meddelanden de skickar till varandra inte ändras under transport utan att det upptäcks. (3p)

(b) Låt m_1 och m_2 vara klartext-meddelanden och H en hash-funktion. För varje egenskap nedan, **motivera kort** om egenskapen är önskvärd eller icke-önskvärd av H.

(1) Om $m_1 = m_2 + m_2$ så ska $H(m_1) = H(m_2) + H(m_2)$. (1p)

(2) Antalet bitar i $H(m_1)$ ska vara exakt lika många som i m_1. (1p)

(3) Det måste existera en funktion H^{-1} sådan att $m_1 = H^{-1}(H(m_1))$. (1p)

Fråga 6: Autentisering (4p)

(a) Beskriv hur en man-in-the-middle attack går till under nyckelutbyte med RSA. (2p)

(b) Förklara hur tidsbaserade lösenord fungerar. (2p)

Fråga 7: Certifikat (4p)

(a) I ett X.509 certifikat, vad finns i fältet *subject*? (1p)

(b) Hur avgör man om ett certifikat är giltigt? Förklara i detalj hela processen. (3p)

Fråga 8: Designprinciper (4p)

Förklara följande designprinciper:

(a) Fail-safe defaults. (2p)

(b) Least privilege. (2p)

Fråga 9: Riskanalys (10p)

(a) Förklara begreppet *analysis paralysis*. (1p)

(b) Trots att CORAS är en kvalitativ metod så kan man ändå estimera risk genom de två faktorerna sannolikhet och konsekvens. Hur? (1p)

(c) Beskriv vad man gör i det femte steget av CORAS? (2p)

(d) Förklara riskanalysmetoden ISRAM. Skapa ett fiktivt scenario där du kan applicera ISRAM och förklara metoden genom att använda den på ditt scenario. Din riskanalys ska inte vara uttömmande, men det ska vara tydligt vad som händer i varje steg. Från din förklaring ska det framgå vilka ekvationer/tabeller som används i varje steg och ges exempel på dessa. (6p)