Försättsblad till skriftlig tentamen vid Linköpings universitet

Datum för tentamen	2017-06-05
Sal (1)	G36(14)
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

2017-06-05

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 innebär det att en säkerhetsmekanism är exakt? (1p)

(b) Ange de två kriterier som måste uppfyllas för att ett system teoretiskt skall vara säkert. (2p)

(c) Förklara begreppen *tillit* och *försäkran* (inom kontexten av säkerhetsmekanismer). (2p)

Fråga 2: Kryptoteknik (10p)

(a) Förklara hur man tar fram de publika och privata nycklarna i RSA, samt hur man krypterar och dekrypterar meddelanden. (3p)

(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) När och varför använder man pseudorandom number generators? (1p)

(d) Kryptera de två meddelandena 0101000111 och 1101010101 med one time pad. (1p)

(e) Varför använder man en initialisation vector? (1p)

Fråga 3: Accesskontroll (4p)

Givet tre klienter C_1, C_2 och C_3 (subjekt) samt två servrar S_1 och S_2 (objekt), skapa en accesskontrollmatris och en access control list för detta system så att policyn nedan uppfylls. (4p)

- C_1 får läsa (r), skriva (w) och exekvera (x) kod på S_1.
- C_2 får läsa och skriva kod på S_2.
- C_2 får skriva kod på S_1.
- C_3 får läsa och exekvera kod på S_2.
- C_3 får skriva kod på S_1.
- Om inget annat anges så ges inga rättigheter.

Fråga 4: Policymodeller (5p)

Förklara Bell-LaPadula med hjälp av ett exempel. Det är viktigt att ditt svar är tydligt och att du förklarar centrala begrepp. (5p)

Fråga 5: Hash-funktioner (6p)

(a) Redogör för algoritmen som används när man beräknar ett HMAC värde? (3p)

(b) När bör man använda HMAC värden? (1p)

(c) Om $H(m) = c$ är en hash-funktion som ger hash c då man använder den på meddelande m, motivera varför det är olämpligt att använda H för att spara lösenord i en databas om:

- $H(H(m)) = H(m)$ (1p)
- $H(m_1 + m_2) = H(m_1) + H(m_2)$ (1p)

Fråga 6: Autentisering (4p)

(a) Förklara tids- samt challenge-response-baserade engångslösenord (förklara även skillnaderna). (2p)

(b) Ge två exempel på risker med biometrisk autentisering. (2p)

Fråga 7: Certifikat (4p)

(a) Förklara varför certifikat-kedjor behövs och hur de fungerar. (2p)

(b) Hur avgör man om ett certifikat är giltigt? Förklara i detalj hela processen. (2p)

Fråga 8: Designprinciper (4p)

Förklara följande designprinciper:

(a) Principle of least privilege. (2p)

(b) Principle of economy of mechanism. (2p)

Fråga 9: Riskanalys (10p)

(a) Förklara genom ett exempel hur man skapar attack träd (alla byggstenar som vi diskuterat i kursen skall förklaras). (2p)

(b) Beskriv vad man gör i det fjärde steget av ISRAM. (2p)

(c) Förklara riskanalysmetoden CORAS. Skapa ett fiktivt scenario där du kan applicera CORAS 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/dokument som skapas och används i varje steg, och du ska ge exempel på dessa. (6p)