Försättsblad till skriftlig tentamen vid Linköpings universitet

Datum för tentamen	2017-08-21
Sal (1)	TER1(6)
Tid	14-18
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	15:00 samt 17:00
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

2017-08-21

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) Definiera vad en säkerhetspolicy är. (1p)

(b) Man brukar tala om två olika typer av integritet, namnge och förklara dessa. (2p)

(c) Förklara hur man kan öka tilliten till en mekanism. (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) Förklara hur man tar fram en gemensam hemlig nyckel med hjälp av Diffie-Hellman. (3p)

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

(d) När och varför använder man pseudo random number generators (PRNGs)? (2p)

Fråga 3: Accesskontroll (4p)

Givet tre databaser D_1, D_2 och D_3 (subjekt) samt två servrar W_1 och W_2 (objekt), skapa en accesskontrollmatris för detta system så att policyn nedan uppfylls. Därefter skapa både en access control list och en capability list som kan representera accesskontrollmatrisen (skriv tydligt vilken som är vilken). De rättigheter som finns i systemet är läsa (r), skriva (w) och exekvera (x). (4p)

- W_1 får skriva på alla enheter i system.
- W_1 får läsa från D_2.
- W_1 får exekvera på D_1.
- W_2 får läsa från D_1 och skriva till D_2.
- 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) Beskriv ett scenario där man bör använda HMAC värden. (2p)

(b) Om $H(m) = c$ är en hash-funktion som ger hash c då man använder den på meddelande m, avgör (med motivation) om H är en lämplig hash-funktion om:

- $H(H(m)) = H(m)$. (1p)
- Då $m_1 \neq m_2$ så ska antalet bitar vara exakt lika många i $H(m_1)$ som i $H(m_2)$. (1p)
- Det existerar en funktion H^{-1} sådan att $H^{-1}(H(m)) = m$. (1p)
- Antalet bitar i $H(m)$ är oberoende av antalet bitar i m. (1p)

Fråga 6: Autentisering (4p)

(a) Förklara vad autentisering innebär (använd begreppen entity, identitet och subjekt). (2p)

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

Fråga 7: Certifikat (4p)

(a) Förklara varför certificate authorities existerar. (1p)

(b) Förklara varför certifikat-kedjor behövs. (1p)

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

Fråga 8: Designprinciper (4p)

Förklara följande designprinciper:

(a) Principle of fail-safe-defaults. (2p)

(b) Principle of open design. (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 femte steget av CORAS. (2p)

(c) 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/dokument som skapas och används i varje steg, och du ska ge exempel på dessa. (6p)