Försättsblad till skriftlig tentamen vid Linköpings universitet

Datum för tentamen	2016-06-07
Sal (2)	TER2 TER4
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	15:20 samt 16:40
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

2016-06-07

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

(b) Hur skiljer sig ett hot från en attack? (1p)

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

Fråga 2: Kryptoteknik (10p)

(a) Varför används en initialisation vector (IV)? (2p)

(b) Nämn två saker som är viktiga för säkerheten när man använder *one-time pad.* (2p)

(c) Rita och förklara detaljerna för hur ett Feistelnätverk används i DES (detaljerna för hur funktionen F ser ut och fungerar skall inte ingå). (3p)

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

Fråga 3: Accesskontroll (4p)

Ett system består av två databaser, D_1 och D_2, samt två webbservrar, W_1 och W_2. Det finns också två klienter, C_1 och C_2. Låt objekten O vara $\{D_1, D_2\}$, och subjekten S vara $\{W_1, W_2, C_1, C_2\}$. Skapa en accesskontrollmatris och en *capability list* för detta system så att följande policy uppfylls: (4p)

- C_1 och C_2 ska kunna exekvera (x) kommandon på båda webbservrar, samt kunna läsa (r) resultatet av dessa exekveringar.
- W_1 ska kunna läsa (r) från D_2 och skriva (w) till D_1.
- W_2 ska kunna läsa (r) från D_1 och skriva (w) till D_2.
- 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) Redogör för algoritmen som används när man beräknar ett HMAC värde. (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 $m_1 \neq m_2$ så ska *antalet bitar* vara exakt lika många i $H(m_1)$ och $H(m_2)$. (1p)

(2) Om H används två eller flera gånger på m_1 så får aldrig resultatet bli det samma. (1p)

(3) Om m_2 är m_1 i omvänd ordning, så måste också $H(m_2)$ vara $H(m_1)$ i omvänd ordning. (1p)

Fråga 6: Autentisering (4p)

(a) Förklara begreppen *entity* och *principal.* (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 psychological acceptability. (2p)

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

Fråga 9: Riskanalys (10p)

(a) Förklara genom ett exempel hur man skapar attack träd. (2p)

(b) Beskriv vad man gör i det tredje 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 som används i varje steg och ges exempel på dessa. (6p)