Skriftlig tentamen

TDDD82 Projekttermin inklusive kandidatprojekt: Säkra, mobila system

2017-02-24

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) Förklara hur man kan öka tilliten till en säkerhetsmekanism. (2p)

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

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

Fråga 2: Kryptoteknik (10p)

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

(b) Förklara hur man tar fram en gemensam hemlig nyckel med hjälp av Diffie-Hellman. (3p)

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

Fråga 3: Accesskontroll (4p)

Givet två databaser DB_1 och DB_2 (objekt) samt en server S, en mobil klient M och en stationär klient K (objekt), skapa en accesskontrollmatris och en *capability list* för detta system så att policyn nedan uppfylls. (4p)

- S får skriva (w) och läsa (r) från båda databaser.
- M får läsa (r) från S.
- K får läsa (r) och skriva (w) till S.
- M får inte skriva till sig själv, men har för övrigt alla rättigheter på sig själv.
- S har alla rättigheter på sig själv.
- Om inget annat anges så ges inga rättigheter.

Fråga 4: Policymodeller (5p)

Förklara Biba integrity model när *low-water-mark-policy* används. Förklara med hjälp av ett exempel. Det är viktigt att du får med och 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) Ska output från en hash-funktion vara det samma om man använder den på samma input två gånger (motivera kort)? (1p)

(d) Output från en hash-funktion för input 'marcus' skall vara det omvända som för input 'sucram'. Sant eller falskt (motivera kort)? (1p)

Fråga 6: Autentisering (4p)

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

(b) Förklara begreppen *entity* och *principal*. (2p)

Fråga 7: Certifikat (4p)

(a) Varför existerar *certificate authorities*? (1p)

(b) Vad finns i fältet *issuer* på ett vanligt certifikat? (1p)

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

Fråga 8: Designprinciper (4p)

Förklara följande designprinciper:

(a) Separation of privilege. (2p)

(b) Principle of open design. (2p)

Fråga 9: Riskanalys (10p)

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

(b) Beskriv vad man gör i de fjärde och femte stegen 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)