Skriftlig tentamen

TDDD82 Projekttermin inklusive kandidatprojekt: Säkra, mobila system

2016-08-22

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 när man säger att en säkerhetsmekanism är säker (secure)? (2p)

(b) Vad innebär cost-benefit analys? (1p)

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

Fråga 2: Kryptoteknik (10p)

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

(b) Kryptera bokstäverna m (01101101) och a (01100001) med one time pad. (2p)

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

Givet tre processer P_1, P_2 och P_3 (subjekt) samt ett nätverkskort N och en hårddisk H (objekt), skapa en accesskontrollmatris och en *capability list* för detta system så att policyn nedan uppfylls. Ge exempel på ett händelseförlopp som tillåter att P_1 tar emot data från nätverket. (4p)

- P_1 och P_3 får läsa (r) från hårddisken.
- P_2 får exekvera (x) och läsa (r) P_3.
- P_3 får skriva till (w) och läsa från (r) från nätverkskortet.
- P_2 får skriva till (w) hårddisken.
- P_1 får exekvera (x) och läsa (r) P_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 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) 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) $H(m_1) = H(m_2)$ om och endast om $m_1 = m_2$. (1p)
(2) $H(m_1) = H(H(m_1))$. (1p)
(3) Antalet bitar i $H(m_1)$ och $H(m_2)$ får endast vara lika om $m_1 = m_2$. (1p)

Fråga 6: Autentisering (4p)

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

(b) Förklara tids- samt challenge-response-baserade engångslösenord (förklara även skillnaderna). (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 fail-safe defaults. (2p)

(b) Principle of least-privilege. (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 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)