5

Skriftlig tentamen

TDDD82 Projekttermin inklusive kandidatprojekt: Säkra, mobila system

2015-08-24

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 (2p)

(a) Mot vilken hörnsten riktar sig en DoS attack? (motivera) (1p)

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

Fråga 2: Policy och mekanismer (3p)

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

(b) Vad är målet med en säkerhetsmekanism? (1p)

Fråga 3: Riskanalys (2p)

Förklara och ge ett exempel på *cost-benefit* analys. (2p)

Fråga 4: Kryptoteknik (9p)

(a) Förklara hur ett *stream cipher* generellt fungerar. (1p)

(b) Varför används en *initialization vector* (IV)? (1p)

(c) Namnge ett *stream cipher*. (1p)

(d) För alla asymmetriska kryptosystem finns det ett gemensamt problem, vilket? (1p)

(e) Vad är resultatet av $1 \oplus 1$? ($\oplus$ är xor operationen) (1p)

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

Fråga 5: Accesskontroll (5p)

Antag att mängden objekt är $O = \{p, q, t\}$, att mängden subjekt är $S = \{a, b, c\}$ och att mängden rättigheter är $R = \{r, w, x\}$. Låt $x(a, p)$ betyda att a har rättighet x på p.

Skapa en *access control list* och en *capability list* för detta system så att följande policy uppfylls: (5p)

- $\forall s \in S : x(s, p)$
- $w(a, p)$, $w(a, q)$, $w(c, p)$
- $r(b, q)$, $r(c, t)$
- Om inget annat anges så ges inga rättigheter.

Fråga 6: 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 7: 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 $m_1 = m_2$ så ska $H(m_1) = H(m_2)$. (1p)

(2) Antalet bitar i $H(m_1)$ ska vara exakt lika många som i $H(m_2)$ för alla m_1 och m_2. (1p)

(3) Det får inte existera en funktion H^{-1} sådan att $m_1 = H^{-1}(H(m_1))$. (1p)

Fråga 8: Autentisering (2p)

(a) Förklara begreppen *entity* och *principal*. (1p)

(b) Ge ett exempel på var *challenge-response* används i vardagslivet. (1p)

Fråga 9: Certifikat (4p)

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

(b) Hur avgör man om ett certifikat är giltigt? Förklara i detalj hela processen. (3p)

Fråga 10: Designprinciper (4p)

Förklara följande designprinciper:

(a) Least privilege. (2p)

(b) Open design. (2p)

Fråga 11: Riskanalys (10p)

(a) Förklara i detalj steg 3 av CORAS. Vilka personer är involverade, vilka aktiviteter pågår, samt vilka diagram/dokument/tabeller produceras och vad är syftet med dessa. Ge exempel på dessa diagram/dokument/tabeller. (3p)

(b) 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. (7p)