5

Skriftlig tentamen

TDDD82 Projekttermin inklusive kandidatprojekt: Säkra, mobila system

2015-02-27

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) Beskriv två faktorer som påverkar integritet. (1p)

(b) Om en attack raderar en databas, vilken av de tre hörnstenarna inom säkerhet är detta ett brott mot? (motivera) (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) Om en säkerhetsmekanism är *bred* (engelska: broad), vad innebär det? (1p)

Fråga 3: Hot, Attack och Risk (2p)

(a) Förklara begreppen *hot* och *attack*. (1p)

(b) I denna kurs definierade vi *risk* som en ekvation, hur ser denna ekvation ut? (1p)

Fråga 4: Kryptoteknik (9p)

(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 privata och publika nycklar i RSA samt hur kryptering och dekryptering fungerar. Din förklaring skall innehålla matematiska detaljer för varje steg. (5p)

Fråga 5: Accesskontroll (5p)

Tre databaser (DB1, DB2 och DB3) finns på ett nätverk. På nätverket finns även tre klienter (C1, C2, C3). C1 får skriva (w) och läsa (r) från DB1 samt läsa från DB2. C2 får läsa från DB2 och DB3. C3 får skriva till DB2 och DB3. Om inget annat anges så ges inga rättigheter.

(a) Skapa en accesskontrollmatris för detta system och fyll i den så att den givna policyn uppfylls. (1p)

(b) Hur kan C3 skicka ett meddelande till C2 utan att C1 kan läsa detta meddelande? (1p)

(c) Översätt accesskontrollmatrisen till en *access control list* (ACL). (3p)

Fråga 6: Policymodeller (5p)

Förklara Bell-LaPadula. Det är bland annat viktigt att få med: (5p)

- Begrepp: säkerhetsnivå, kategori, klassificering, dominerar.
- Regler för läsning och skrivning.

Fråga 7: Hash-funktioner (6p)

(a) Redogör för algoritmen som används när man beräknar ett HMAC värde? (3p)

(b) Låt m vara ett klartext-meddelanden och H en hash-funktion. För varje egenskap nedan, **motivera kort** om egenskapen är önskvärd eller icke-önskvärd av H.

(1) Om hash-funktionen används två eller fler gånger på m får aldrig resultatet bli det samma, dvs $H(m) \neq H(m)$. (1p)

(2) Det måste existera en funktion H^{-1} sådan att $m = H^{-1}(H(m))$. (1p)

(3) Om jag ändrar en bit i m så skall endast en bit i $H(m)$ förändras. (1p)

Fråga 8: Autentisering (2p)

(a) Vad innebär *flerfaktor-autentisering*? Förklara och ge ett exempel på detta. (1p)

(b) Förklara vad *challenge-response* innebär. (1p)

Fråga 9: Certifikat (4p)

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

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

Fråga 10: Designprinciper (6p)

Förklara följande designprinciper:

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

(b) Psychological acceptability. (2p)

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

Fråga 11: Riskanalys (8p)

(a) Redogör för proceduren man skall följa när man skapar attack-träd. (2p)

(b) Redogör för riskanalysmetoden CORAS. För varje steg förklara: 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. (6p)