Skriftlig tentamen

TDDD82 Projekttermin inklusive kandidatprojekt: Säkra, mobila system

2015-06-08

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) Namnge och förklara tre grundläggande säkerhetsbegrepp inom säkerhet. (1p)

(b) Om en attack bryter strömmen till en server, vilken av de tre hörnstenarna inom säkerhet är detta ett brott mot? (motivera) (1p)

Fråga 2: Policy och mekanismer (3p)

(a) Vad är en säkerhetspolicy? (1p)

(b) Förklara skillnaden mellan en *bred* (en: broad) och en *säker* (en: secure) säkerhetsmekanism? (2p)

Fråga 3: Hot, Attack och Risk (2p)

Förklara och ge exempel på hur man kan jämföra två kvalitativa risker. (2p)

Fråga 4: Kryptoteknik (9p)

(a) Förklara två saker som är viktiga för säkerheten när man använder one-time pad. (1p)

(b) Namnge ett symmetriskt och ett asymmetriskt kryptosystem. (1p)

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

(d) Måste de två initiella primtalen hållas hemliga när man genererar nycklar i RSA? (1p)

(e) Förklara Diffie-Hellman processes, din förklaring skall innehålla fullständiga matematiska detaljer. (5p)

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.

(a) Skapa en accesskontrollmatris för detta system och fyll i den så att följande policy uppfylls: (2p)

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

(b) 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) Vilken av säkerhetens hörnstenar används i huvudsak hash-funktioner till? (motivera) (1p)

(b) Hur skiljer sig HMAC från vanliga hash-funktioner? (1p)

(c) Namnge två hash-funktioner (ej HMAC). (1p)

(d) 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 aldrig vara lika många i $H(m_1)$ och $H(m_2)$. (1p)
(2) $H(m_1 + m_2) = H(m_1) + H(m_2)$. (1p)
(3) Det måste 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 två exempel på risker med biometrisk autentisering. (1p)

Fråga 9: Certifikat (4p)

(a) Varför behövs certifikatkedjor? (1p)

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

Fråga 10: Designprinciper (4p)

Förklara följande designprinciper:

(a) Economy of mechanism. (2p)

(b) Fail-safe defaults. (2p)

Fråga 11: Riskanalys (10p)

(a) Redogör för proceduren man skall följa när man skapar attack-träd. (3p)

(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. (7p)