Mittuniversitetet
MID SWEDEN UNIVERSITY

Tentamen

DT012G Informationssäkerhet och riskanalys

Daniel Bosk
daniel.bosk@miun.se
Telefon: 060-14 8709

2013-06-03

Instruktioner

Läs uppgifterna noggrant innan du börjar att lösa dem. Läs igenom samtliga uppgifter innan du börjar att lösa den första. Planera din skrivning utifrån den tidsbegränsning som anges nedan. Besvara endast frågan, skriv inte svar som ej är relaterad till frågan.

Tänk på att skriva med ett korrekt språk; grammatik och meningsbyggnad är viktigt. Svaret ska tydligt framgå. Dina svar ska visa att du förstått, tänk på att utforma dem för att visa just detta.

Frågorna är *ej* sorterade efter svårighetsgrad.

Lärare finns tillgänglig via telefon under tentan. Svar på frågor som läraren anser berör samtliga kommer att publiceras i kursens diskussionsforum. Notera att diskussionsforumet ej kommer att övervakas under denna tentamen, ställ därför inga frågor där.

Skrivtid 3 juni 2013 kl. 13:00 till kl. 19:00. (6 timmar, inkl. kortare paus).

Hjälpmedel Kurslitteratur, egna anteckningar och referensmaterial på webben.

Antal uppgifter 6

Antal poäng 39

Betygssättning

Denna tentamen betygsätts med betygen A, B och F. För slutbetygen E, D och C krävs inte denna tentamen, då räcker att du är godkänd på samtliga obligatoriska inlämningsuppgifter samt projekt.

Slutbetyget baserar sig på medelbetyget från de obligatoriska momenten. Om du får ett B på denna tentamen ökas ditt slutbetyg med ett betygsteg. På samma sätt om du får ett A ökas ditt slutbetyg med två betygsteg.

Preliminära betygsgränser för B är minst 50 % och för A krävs minst 90 %.

Uppgifter

Nedan följer uppgifterna, glöm inte att de är givna utan inbördes ordning.

1. Universitetets lösenordspolicy kräver minst åtta tecken. Dessa tecken ska vara minst tre gemener, tre versaler och två siffror – dessutom måste dessa finnas bland de första åtta tecknen i lösenordet. Detta ger $26^3 26^3 10^2 = 26^6 10^2 \approx 2^{35}$ antal möjliga lösenord. Lösenordet måste dessutom bytas var tredje månad, vilket i sin tur ger risken för lösenordssystem där användaren baserar det nya lösenordet på det gamla.

   Den något enklare lösenordspolicyn minst åtta tecken med gemener, versaler och siffror – utan krav på något antal inom de olika kategorierna – ger $(26 + 26 + 10)^8 = 62^8 \approx 2^{48}$ antal lösenord. Denna policy har inga krav på giltighetstid hos ett lösenord.

   Resultatet av detta är en reduktion av komplexiteten från 62^8 ned till $26^6 10^2$. Detta utgör en relativ minskning av komplexiteten med $1 - \frac{26^6 10^2}{62^8} = 0.99986$, alltså 99.99 procent.

   Oavsett vilken av ovan givna policyer som används får användarna svaga lösenord.

(4p) (a) Förklara hur dessa lösenordspolicyer kan angripas.

(4p) (b) Ge ett förslag på en riktigt bra lösenordspolicy. Förslag utan motivering ger noll poäng.

2. Definiera följande begrepp:

(1p) (a) pålitlighet (trust),

(1p) (b) pålitlig (trustworthy),

(1p) (c) sekretess (secrecy),

(1p) (d) konfidentialitet (confidentiality),

(1p) (e) personlig integritet (privacy),

(1p) (f) integritet (integrity), och

(1p) (g) autenticitet (authenticity).

3. Människans psykologi spelar en stor roll för säkerheten hos olika system.

(2p) (a) Förklara översiktligt varför psykologin är viktig inom säkerhetsområdet.

(4p) (b) Analysera en psykologibaserad attack och förklara varför den fungerar.

(4p) 4. Definiera begreppet mannen-i-mitten-attack (man-in-the-middle attack) och illustrera begreppet med ett exempel.

5. Flernivåsäkerhet (multi-level security) och multilateral säkerhet (multi-lateral security) är två relaterade begrepp.

(4p) (a) Vad innebär flernivåsäkerhet? Förklara vad som ämnas med detta.

(4p) (b) Vad innebär multilateral säkerhet? Förklara vad som ämnas med detta.

(2p) (c) Beskriv fördelarna med att kombinera de båda metoderna.

(4p) 6. Beskriv problemen som kan uppstå med biometriska system och förklara hur dessa kan användas trots dessa begränsningar.