Bokmål

Norges teknisk-naturvitenskapelige universitet
Institutt for telematikk

KONTINUASJONSEKSAMEN I
TTM4135 – INFORMASJONSSIKKERHET

Faglig kontakt under eksamen: Professor Stig F. Mjølsnes. (tlf. 413 05 114).

Eksamensdato: 16. august 2005.

Eksamenstid: kl. 15:00 – 19:00 (4 timer).

Sensurdato: 7. september 2004.

Studiepoeng: 7,5

Tillatte hjelpemidler: Kalkulator. Ingen trykte eller håndskrevne hjelpemidler tillatt (D).

Vedlegg: 2 sider med eksamensoppgaver.

Dette oppgavesettet består av 32 oppgaver oppdelt i fire deler. Vektlegging er angitt i prosent i deloverskriftene og i parentes i enden på enkeltspørsmålene. Eksamensoppgavene kommer ikke nødvendigvis i økende vanskelighetsgrad for deg, så planlegg tiden slik at du får mulighet til å svare på alle oppgavene. Vennligst gjør ditt beste til å skrive konsist og med skjønn skrift!

Del I (40 %) Begreper og fakta.

Gi en kort definisjon/forklaring på hvert av de følgende begrepene og forkortelsene i informasjonssikkerhet: (2 % hver)

1. Autentisering.
2. Asymmetrisk kryptosystem.
3. Digitalt sertifikat.
4. Datavirus.
5. Dataorm.
6. HMAC.
7. Informasjonsteoretisk sikkerhet.
8. Nonce (engelsk.).
9. X.509.
10. Gjentaksangrep.
11. SNMP MIB.
12. ISAKMP.
13. PGP.
14. Kerberos.
15. S/MIME.
16. AES.
17. Vernam-chiffer.
18. SHA.
19. IPsec ESP.
20. crypt(3)

Del II. (20 %) Kryptografi

21. Det symmetriske blokkchifferet DES har "Feistel-struktur". Hva kjennetegner en Feistel-struktur? (2 %)
22. Vis algebraisk at en Feistel-kryptering alltid er inverterbar. (4 %)
23. Beskriv følgende operasjonsmodi for blokk-chiffer, både kryptering og dekryptering: (6 %)
    1) ECB
    2) CBC
    3) CFB

Konseptet med beregningsmessige enveisfunksjoner er fundamentalt for moderne kryptografiske prinsipper.

24. Gi en matematisk definisjon av beregningsmessige enveisfunksjoner. (5 %)
25. Presenter en tall-teoretisk funksjon som tilfredstiller definisjonen i oppgaven foran, og forklar hvordan denne beregnes. (3 %)

Del III. (30 %) Hærverksprogramvare

Programvare kan med hensikt konstrueres med skjult funksjon som gjør skadeverk.

26. Presenter en oversikt over kategorier av slik programvarefunksjonalitet. (4 %)
27. Forklar viktige forskjeller mellom *pålitelig (eng. reliable)* og *sikker (eng. secure)* programvare. (6 %)

28. Forklar oppførselen til følgende program: (6 %)

```
Program V := {
     goto dmg;
     1234567;
     subroutine infect-executable := {
          loop:     file := get-random-executable-file;
               if (second-line(file) = '1234567')
               then goto loop
               else prepend V to file;}
     subroutine do-damage := {
          whatever_is_to_be_vandalised}
     subroutine trigger-pulled := {
          return(test_some_condition)}
dmg: infect-executable;
     if trigger-pulled then do-damage;
}
```

29. Det er programmert en ”evig løkke” i V, påpek denne? (4 %)
30. Anta at vi har et program D som kan analysere og bestemme om programvare har skadeverksoppførsel. Det vil si, for en hver programkode P som input, dersom vi kjører D(P) så vil D returnere verdien TRUE dersom ”P er et software virus”, ellers returnerer D verdien FALSE. Se så på følgende programskisse W:

```
Program W :={
   ... other_necessary_code...
        if D(W) then goto nothing
        else infect-executable;
nothing:
}
```

Subrutine `infect-executable` er lignende til den vist i program V. Diskuter om D kan korrekt bestemme om W vil oppføre seg ødeleggende, og forklar de logiske konsekvensene av din argumentasjon. (10 %)

Del IV. (10 %) Kryptoprotokoller

Alice og Bob har allerede blitt enige om å benytte Diffie-Hellman nøkkelutvekslingsprotokollen med 18 som generator i den multiplikative gruppen Z^*_{3061}, hvor 3061 er primtall. I en utførelsesinstans av protokollen mottar Bob tallet 349 fra Alice, deretter velger Bob tilfeldig tallet 12. Anta at alt forløper korrekt etter protokollen, og vis eksplisitt beregningene som gjøres i det følgende:

31. Hvilket tall sender Bob til Alice? (5 %)
32. Hvilket tall blir deres delte hemmelighet? (5 %)