Bokmål

Norges teknisk-naturvitenskapelige universitet
Institutt for telematikk

EKSAMEN I
TTM4137 – INFORMASJONSSIKKERHET i MOBILNETT

Faglig kontakt under eksamen: Professor Stig F. Mjølsnes. (mobil 918 97 772).

Eksamensdato: 16. desember 2011.

Eksamenstid: kl. 9:00 – 13:00 (4 timer).

Sensurdato: 16. januar 2012.

Studiepoeng: 7,5

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

Vedlegg:

- 6 sider med eksamensoppgaver
- 1 besvarelsesark for Del 1

Oppgavesettet består av 35 oppgaver inndelt i 3 deler. Vektlegging er angitt i prosent i avsnittsoverskriftene, og fordelt på enkeltspørsmål der det er aktuelt. Eksamensoppgavene kommer muligens, men ikke nødvendigvis i økende vanskelighetsgrad for deg, så planlegg tiden slik at du får mulighet til å svare på alle oppgavene. Forsøk helst å lage kortfattede svar. Vi vil sette stor pris på at du skriver forståelig og med skjønn skrift. Lykke til!

Del I. Fakta om sikkerhet i trådløse nett. (50%)

Denne delen består av 25 flervalgsoppgaver, med likt fordelt vekt på alle spørsmålene. Hvert spørsmål har fire mulige svar, men bare ett av disse er riktig. Riktig svar gir 2 poeng, mens dobbeltsvar, feil eller manglende svar gir null poeng. *Bruk vedlagte svarark for denne delen.*

1. Hvilken store svakhet i WEP utnyttes av PTW-angrepet som vi benyttet i lab-øvingen?
   a) Initialiseringsvektoren er for kort
   b) Ingen beskyttelse mot meldingsrepetisjon
   c) Integritetsjekksummen er for kort
   d) IV-verdien er del av nøkkelstrømmen
2. Hva er lengden av WEP initialiseringsvektor (IV)?
   a) 24 bits
   b) 32 bits
   c) 48 bits
   d) 64 bits
3. Hvordan transporteres EAP-meldinger mellom autentikatoren og autentiseringstjeneren i RSN?
   a) EAP-meldingene er innkapslet i TCP/IP
   b) EAP-meldingene er innkapslet i EAP-TLS
   c) EAP-meldingene er innkapslet i VPN
   d) EAP-meldingene er innkapslet i 801.1X
4. Hvilken kryptoalgoritme brukes på tellermåte med kryptoblokklenking for meldingsautentiseringskode i CCMP?
   a) AES
   b) Michael
   c) RC4
   d) KASUMI
5. Hva er hensikten med EAPOL 4-veis håndtrykk?
   a) Beregne en fersk pairwise temporal key (PTK) fra pairwise message key (PMK)
   b) Beregne en fersk pairwise master key (PMK) fra pairwise transient key (PTK)
   c) Beregne en fersk pairwise transient key (PTK) fra pairwise master key (PMK) etter at begge parter har verifisert PMK
   d) Beregne en fersk pairwise message key (PMK) fra pairwise trusted key (PTK) generert i 4-veis nøkkelavtaleprotokoll
6. Hvordan fungerer et blokkchiffer i tellervirkemåten?
   a) $C = E(i) \oplus i$
   b) $C = E(i) \oplus M \oplus i$
   c) $C_i = E(i) \oplus M_i$
   d) $C = E(i) \oplus M$

7. Er hele MAC PDU kryptert i CCMP?
   a) Ja, CCMP bruker en delt nøkkel
   b) Ja, CCMP-hodet er kryptert
   c) Nei, MAC-hodet er ikke kryptert
   d) Nei, MAC-hodet og CCMP-hodet er ikke kryptert
8. Hvilken virkemåte brukes blokkchifferet AES på i RSN?
   a) Tellermåte med chifferblokklenket meldingsautentiseringskode
   b) Tellermåte med Galois meldingsautentiseringskode
   c) Chifferblokklenking med tellermåte meldingsautentiseringskode
   d) Chifferblokklenking med krystet meldingsautentiseringskode
9. Hvordan blir den 128 bits startverdien i telleren for CCMP-kryptering initialisert i RSN?
   a) Med en tilfeldig IV
   b) Med å sette sammen IV og den utvidete IV
   c) Med flag/priority bits, packetnumber, source-address, og en konstant
   d) Med source address, destination address og MIC-verdi av MPDU
10. Hvilken 802.11 rammetype er kryptografisk beskyttet i 802.11w standarden?
    a) Datarammer
    b) Controlrammer
    c) Managementrammer
    d) Beaconrammer
11. Hvordan beskytter UMTS mot avlytting av abonnentsidentifikatoren over radiokanalen?
    a) Ved at nettet forsyner midlertidige abonnentsidentiteter til USIMene
    b) Ved å beholde abonnentsidentitet inne i USIM
    c) Ved å lagre den 128-bits hemmelige nøkkelen (K_{IMSI}) i USIMen og bare distribuere til tiltrodde VLRer.
    d) Ved å bruke IMEI istedet for IMSI
12. Hvilken informasjon sendes fra HSS til MME i løpet av LTE/EPS-autentiseringsprotokollen?
    a) IMSI, RAND, AUTN, XRES
    b) RAND, AUTN, XRES, K_{ASME}
    c) RAND, AUTN, XRES, CK, IK
    d) RAND, AUTN, XRES, K_c
13. Hvilket UTRAN protokollag utfører kryptering?
    a) MAC-laget og RRC-laget
    b) RLC-laget og RRC-laget
    c) PHY-laget og MAC-laget
    d) MAC-laget og RLC-laget

14. Hva skjer dersom UTRAN forhandlingsprotokoll for kryptoalgoritmer finner at brukerutstyret (UE) og nettet ikke har noen felles krypteringsalgoritme?

    a) UTRAN sender en ny krypteringsalgoritme som en app-nedlasting
    b) UTRAN kobler ned forbindelsen umiddelbart
    c) UTRAN kan velge å etablere forbindelsen uten kryptering
    d) UTRAN bruker ikke kryptoalgoritme-forhandling

15. I hvilken operasjonsmåte brukes KASUMI for å konstruere 3GPP $f8$ nøkkelstrømsgeneratoren?

    a) Kombinasjonen Counter-mode og ECB-mode
    b) Kombinasjonen Counter-mode og CCM-mode
    c) Kombinasjonen Counter-mode og OFB-mode
    d) Kombinasjonen Counter-mode og CBC-mode

16. Hva er den underliggende antakelsen i sikkerhetsanalysen av MILENAGE ?

    a) Ingen antakelser ble gjort
    b) Kjernefunksjonen må være et sikkert blokkchiffer
    c) AES må benyttes som kjernefunksjon
    d) Kjernefunksjonen må være en enveisfunksjon

17. Hvorfor kan UICC normalt enkelt demonteres fra UE?

    a) UE produksjons- og bruksløp kan gjennomføres uavhengig av brukertilknytning og abonnementsprosess
    b) Feilraten til smartkort (UICC) er høy fordi utstedere (mobiloperatørene) ønsker å redusere kostnad for kortere abonnementsvarighet
    c) Ende-til-ende UMTS nøkkelkort kan dermed settes inn i USIM-inngangen for nøkkeldistribusjon and -administrasjon
    d) USIM inneholder en utløpsdato, på samme måte som et kredittkort, og må kunne erstattes med nytt

18. Hva er bitlengden på den faste abonnentsnøkkelen i UMTS?

    a) 56
    b) 64
    c) 128
    d) 256

19. Endepunktene for krypterte brukerdata over EPS er

    a) UICC og eNB
    b) UE og MME
    c) UE og eNB
    d) UICC og MME

20. Endepunktene for krypterte signalmeldinger i EPS AS er
    a) UICC og eNB
    b) UE og eNB
    c) eNB og MME
    d) UE og MME
21. Endepunktene for krypterte signalmeldinger i EPS NAS er
    a) UICC og eNB
    b) UE og eNB
    c) eNB og MME
    d) UE og MME
22. Kan LTE/EPS tilby end-til-ende datasikkerhet?
    a) Nei
    b) Ja, men bare autentisitet
    c) Ja, men bare anonymitet
    d) Ja, både konfidensialitet og autentisitet
23. Kan en 3G USIM virke i et LTE/EPS UE håndsett?
    a) Nei, fordi krypto-nøklene må beholdes i USIM
    b) Nei, fordi krypto-nøklene er ikke kompatible
    c) Ja, fordi krypto-nøklene er de samme i begge systemene
    d) Ja, fordi USIM nøkkel utdata er det samme i begge systemene
24. Hvor ligger nøkkelavledningsfunksjonen KDF i EPS?
    a) I USIM og AuC
    b) I USIM og UE
    c) I UE og MME
    d) I UE og HSS
25. Hva er lovlig avlytting i mobikommunikasjonsnett?
    a) Avlytting godkjent av lovlig rettsinstans
    b) Avlytting utført av eller på vegne av politiet
    c) Signal-jamming beordret av politimyndighet
    d) Politiets ordre til mobiloperatør om å skru av kommunikasjonskryptering slik at avlytting blir mulig

Del II. Kryptografiske mekanismer (35%)

26. Hva er forskjellen på et blokkchiffer og et strimchiffer? (3%)

27. Hva er en enveis-funksjon? Gi ett eksempel på en enveis-funksjon konstruksjon, og hvordan denne kan brukes? (4%)

28. Definer chifferblokklenkingsmåte med en algebraisk formulering for blokkchifferet $c = e_k(m)$. (3%)

29. Hva er en meldingsautentiseringskode (MAC)? Gi et eksempel på en konstruksjon av en MAC-funksjon. (5%)

30. Kan du finne en god grunn for å bruke MD5 krystefunksjonen[1] slik det gjøres i digital etterforskning, istedet for å benytte autentiseringskoder (MAC) for å identifisere kjente filer. (3%)

31. Hva er hensikten med en initaliseringsvektoren (IV). Hvor stor må mengden av IV-verdier være, og hvordan kan verdiene velges? (7%)

32. Analyser pseudokoden for RC4-algoritmen nedenfor og beregn hvor stort nøkkelrommet kan bli? Forklar. (4%)

Variables:

```
int keylength
byte i, j, S[256], keyinput[int]
boolean Continue
```

RC4 key schedule:

```
for i from 0 to 255
   { S[i] := i }
j := 0
for i from 0 to 255
  { j := (j + S[i] + keyinput[i mod keylength]) mod 256
   swap(S[i], S[j]) }
```

RC4 generator:

```
i := 0 ;  j := 0 ; Continue := True
while Continue  {
    i := (i + 1) mod 256
    j := (j + S[i]) mod 256
    swap(S[i], S[j])
    output S[(S[i] + S[j]) mod 256] }
```

33. En pseudorandom-generator kan modelleres som en tilstandsmaskin. Hva er antallet mulige tilstander for RC4-generatoren? Hva kan du se ut av *forholdet* mellom antall mulige tilstander og nøkkelrommet til RC4. (En sidebemerkning: Antall atomer i det observerte universet er estimert til 10^{80}, et forsvinnende lite antall i denne sammenhengen!) (6%)

[1] Jada, fullstendig nytt norsk ord for hash function! Kommentarer mottas.

Part III. Protocols (15%)

34. Nevn og karakteriser hovedtypene av protokollangripere, og ranger dem etter deres evner til angrep. (5%)

35. Konstruer en kryptoprotokoll mellom to parter som ønsker å velge og bruke en utav mange mulige MAC-algoritmer, over et åpent og usikkert nett. Forklar modellen og antakelser, protokollangriperkategorier, meldingsutveksling, lokale beregninger, og uttrykk punktvis dine sikkerhetspåstander for protokollen. (10%)

sfm