Johan Karlander, CSC, KTH

Tentamen i DD2495, Nätverkssäkerhet

2011 - 05 - 23 Kl 14.00 - 19.00

Inga hjälpmedel är tillåtna.

Tentan består av två delar. Den första delen består av 10 uppgifter som rätt besvarade ger 1 poäng och felaktigt besvarade eller obesvarade ger 0 poäng. För att få godkänt på tentan krävs att du får minst 6 poäng på del 1 (oberoende av resultat på del 2). Poängen från del 1 adderas till poängen från del 2. Betyg sätts enligt skalan:

E: $15 \leq x \leq 19$
D: $20 \leq x \leq 24$
C: $25 \leq x \leq 29$
B: $30 \leq x \leq 34$
A: $35 \leq x$

Del 1 Följande uppgifter skall besvaras sant eller falskt. I de fall då du eventuellt är osäker på ditt svar kan du lämna en *kort* motivering. Uppgifterna ger 1 poäng var.

1. Ett problem med Needham-Schroeder är att KDC inte autentiserar sig för klienterna.
2. Om man använder AES i CBC-mode och man gör en lokal ändring i kryptotexten så kommer denna ändring att fortplanta sig i hela klartexten vid dekryptering.
3. IPSec kommer att gå att använda med Ipv6.
4. Om man använder nonce i ett autentiseringsprotokoll måste dessa nonce nödvändigtvis vara slumpmässigt valda för att man skall få säkerhet.
5. En skillnad mellan DES och AES är att DES är konstruerat med delvis dolda designkriterier medan AES är konstruerat med öppna designkriterier.
6. Det finns en PKI-modell i vilken man tillåter att en kedja av certifikat får bilda en cykel.
7. SSL använder sig av RSA.
8. I Kerberos måste en klient autentisera sig för TGS vid varje ny kontakt.
9. WPA betraktas inte längre som säkert för WiFi.
10. IKE använder sig av cookies.

Del 2

1. (4 p)
   Vi vet att systemen DES och AES båda är *ickelinjära*. Vi skall i den här uppgiften försöka förklara varför det är så. Antag att kryptofunktionen, som kan vara DES eller AES, skrivs som E och att vi har $E(M, K) = C$. Vi kan nu tänka oss två urartade fall: Först att $M = 0$ d.v.s. strängen som bara består av nollor och sedan att $K = 0$.

   Förklara tydligt, genom att beskriva lite om DES och AES konstruktion, varför vi *inte* får $E(0, K) = 0$ och $E(M, 0) = M$.

   Ger värdet på $E(M, 0)$ och $E(0, K)$ någon uppenbart känslig information?

2. (5 p)
   SSL använder sig av en speciell metod för att generera nycklar. Metoden är att K sätts till $K = f(R_1, R_2, S)$ där f är en typ av hashfunktion och R_1, R_2, S är olika slumptal som genereras i protokollet.

   a. Beskriv vad de olika slumptalen är och hur de dyker upp i SSL-protokollet.

   b. Antag nu att en angripare lyckats få tag i ett par strängar M, C där C är M krypterat med den hemliga nyckeln K. Antag att angriparen vill försöka leta fram nyckeln K med en Brute Force-metod. Hur skulle han kunna göra det? En möjlighet är att testa med alla nycklar K. En annan metod är att vi antar att angriparen känner till f och att han försöker generera alla tänkbara nycklar genom att testa att beräkna $f(R_1, R_2, S)$ för alla möjliga värden på parametrarna.
   Avgör under vilka omständigheter den första metoden bör vara effektivast och under vilka omständigheter den andra bör vara effektivast.

3. (4 p)
   Vi har två datorer A och B. Vi vill upprätta en förbindelse mellan dem. Vi tänker oss att denna förbindelse skall gå över två routrar R_1 och R_2 där A har en förbindelse med R_1 och B har en förbindelse med R_2. Vi tänker oss att förbindelsen mellan R_1 och R_2 skall vara säker och använder därför IPSec. Vi vill att förbindelsen skall ge konfidentialitet och integritet. Förklara hur IPSec lämpligen används för att åstadkomma detta.

4. (5 p)
   Vi tänker oss att vi har en användare A som vill kommunicera med en bank B. Det är ordnat så att förbindelsen sker med symmetrisk kryptering och så att man använder en KDC. Om A vill skicka ett meddelande M till B gör han det i följande steg.

   (a) A genererar en nyckel K_{ab}.
   (b) A använder sin nyckel K_a som används för kommunikation med KDC och skickar "$A, \{B, N_1, K_{ab}\}_{K_a}$" till KDC.
   (c) KDC skickar "$\{A, N_1, K_{ab}\}_{K_b}$" till B och skickar "$\{N_1\}_{K_a}$" till A.
   (d) A skickar "$\{M, N_1\}_{K_{ab}}$" till B.

   Vad tycker du om det protokollet? Verkar det ha några svagheter? Tänk dig följande scenario. Den onde T har utfört ett jobb åt A och skall få 500 kr för det (löjligt lite). T vet att A kommer att kontakta banken B och ge den i uppdrag att betala ut pengarna till T. Ange en attack som T skulle kunna genomföra. Ange under vilka antaganden attacken skulle kunna lyckas. Ange slutligen lämpliga motmedel mot attacken.

5. (4 p)
Vi skall titta på några frågor om certifikat (som i RSA). Vi kan förenklat tänka på certifikat som en sträng $T, Sign$ där $T = A, B, K_a^+$ och $Sign = \{H(T)\}_{K_b^-}$. Här är H någon lämplig hashfunktion. Vi tänker oss nu att vi har tre fall som kan verka överraskande och potentiellt farliga. Avgör för de tre fallen hur det kan komma sig att situationen uppstått, om den är säkerhetsmässigt farlig och då på vilket sätt.

   a. Två certifikat är signerade med samma privata nyckel d.v.s. $K_{b_1}^- = K_{b_2}^-$. (Men $b_1 \neq b_2$.)
   b. Två certifikat innehåller samma publika nyckel d.v.s. $K_{a_1}^+ = K_{a_2}^+$. (Men $a_1 \neq a_2$.)
   c. Två certifikat har samma certifikat d.v.s. $Sign_1 = Sign_2$. (Men $T_1 \neq T_2$.)

6. (5 p)
I Kerberos 4 används något som kallas autentiserare (authenticator). Den har grovt sett formen $\{X\}_K$ d.v.s. något är krypterat med en nyckel. Vad är det för något som är krypterat och vilken nyckel är det? En autentiserare är kopplad till en biljett och skall visa att innehavaren är den rätta innehavaren av biljetten. Hur går det till? Vad händer om någon stjäl biljetten och autentiseraren? Kan han göra en replay-attack?

7. (3 p)
Här följer tre frågor rörande kapitel 26. Rättare sagt är det några begrepp som du bör resonera kring vad de innebär och hur viktiga de är.

   a. Perfect Forward Security. Vad innebär det och hur viktigt är det?
   b. Använd olika nycklar för kryptering och signering?
   c. Slumptalsgeneratorer som hårdvara och inte som mjukvara? Vad är lämpligt och varför?