Lösningsförslag till tenta i DD2495, Nätverkssäkerhet

2012-06-01

Del 1

1. Falskt.
2. Sant.
3. Falskt.
4. Falskt.
5. Sant.
6. Sant.
7. Sant.
8. Sant.
9. Sant.
10. Falskt.

Del 2

1. När vi ändrar ett block X_1 kommer ändringen generellt att fortplanta sig genom hela sviten av krypterade block. Om vi däremot ändrar i Y_1 kommer ändringen aldrig att påverka mer än blocken X_1 och X_2.
2. Man kan göra så att första gången A kontaktar B skickar hon $H^{n-1}(L)$. B kan beräkna hashvärdet av detta och se om det är $H^n(L)$. Han sparar sedan $H^{n-1}(L)$. När A kontaktar B gång k skickar hon $H^{n-k-1}(L)$ och B beräknar hashvärdet och ser om det är $H^{n-k}(L)$ o.s.v. Denna metod brukar kallas Lamports hash. Den skyddar mot två olika attacker: Dels replay-attacker och dels attacker som bygger på att en angripare bryter sig in hos B och finner $H^{n-k}(L)$.
3. De modeller som framför allt bör nämnas är monopolmodellen, oligarkimodellen och anarkimodellen. För beskrivning av dessa se läroboken kap 15.

4. Det fullständiga protokollet ser ut så här:

$$
\begin{aligned}
&1. C \rightarrow AS: \ ID_C, ID_{tgs} \\
&2. AS \rightarrow C: \ K_C(Ticket_{tgs}) \\
&3. C \rightarrow TGS: \ ID_C, ID_V, Ticket_{tgs} \\
&4. TGS \rightarrow C: \ Ticket_v \\
&5. C \rightarrow V: \ ID_C, Ticket_V
\end{aligned}
$$

   $Ticket_{tgs}$ används när klienten skall kontakta TGS-servern. $Ticket_V$ används när klienten kontaktar en viss server V. Biljetten innehåller information om användarnamn, servernamn, användarens nätverksadress, biljettens livstid och lite till. Den är krypterad med mottagande serverns hemliga nyckel.

5. Det första läget kallas transportläge och det andra kallas för tunnelläge. Transportläge användes för att skicka meddelanden mellan två användare (ändpunkter). Tunnelläge används för att skicka meddelanden mellan två gateways. I transportläge skickas adressen helt öppet. I tunnelläge är originaladressen krypterad och istället skickas en ny IPheader med adressen till motsvarande gateway helt öppet.

6. a. Nyckeln konstrueras enligt $K = f(S, R_A, R_B)$ där S är en hemlighet som genereras av A och som skickas till B krypterad med en public key-mekanism. R_A och R_B är nonces som genererats av A och B i inledningen av kommunikationen.

   b. I SSLprotokollet talar användarna om den senaste version av SSL som de stödjer. Attacken som beskrivs handlar om att en fiende kan lura två parter att kommunicera med ett onödigt svagt protokoll (och därmed kan utnyttja protokollets svagheter). Svagheten som utnyttjas är att versionsnumret skickas i klartext i inledningen av sessionen.Motmedlet är kortfattat att klienten i ett senare skede skickar en krypterad bekräftan på versionsnumret.

7. Här är några kortfattade förslag på svar.

   a. Det finns huvudsakligen ett skäl som talar för principen. Det är att om meddelandet är långt så kan checksumman beräknas medan meddelandet skickas (och mottas).

   b. Ett skäl som talar för är att ett komprimerat meddelande är Ett kryptografiskt skäl för är t.ex. att Brute-Force-attacker blir svårare att genomföra eftersom det är svårt att känna igen en komprimerad klartext. Men det är inte helt klart att det alltid behöver vara så.

   c. I viss mån gäller att ett krypterat meddelande inte skall kunna förvanskas på ett kontrollerat sätt. Men t.ex. för ett blockchiffer har vi i uppgift 2 sett att det inte är riktigt sant. I boken finns det också på

sid 665 beskrivet en typ av attack mot ett system som bara använder kryptering. Det är hur som helst enkelt att skicka $E(M)E(H(M))$ istället för bara $E(M)$ och det är att rekommendera.