Paar & Pelzl, Capítulo 13

Protocolos de acordo/troca de chaves
Kerberos, autenticação e selos temporais
Diffie-Hellman, ataque do homem-no-meio
Infraestruras de chaves públicas, certificados digitais

Exercícios

Exercício 1
Neste exercício pretende-se analisar variantes que permitam de uma chave mestra CM (que foi partilhada a priori de forma segura usando DH) gerar chaves de sessão que são atualizadas frequentemente. Considere os seguintes métodos para o fazer:
(1) k(0) = CM; k(i+1) = k(i)+1
(2) k(0) = h(CM); k(i+1) = h(k(i))
(3) k(0) = h(CM); k(i+1) = h(CM,i,ki)
em que h é uma função difícil de inverter e , denota concatenação.
1. Quais são as grandes diferenças entre estes processos?
2. Qual destes garante que mesmo que uma chave de sessão seja descoberta, as mensagens trocadas anteriormente não são reveladas?
3. Assuma que Oscar obtém a n-ésima chave de sessão. Para cada caso, que sessões ficam comprometidas, i.e., quais as sessões que se podem decifrar?
4. Que métodos permanecem seguros se a chave mestra ficar comprometida?

Exercício 2
Imagine uma rede com 1000 utilizadores que querem comunicar entre si de forma confidencial e autenticada.
1. Quantas chaves são necessárias trocar para que todos comuniquem uns com os outros sem recurso a uma entidade reguladora usando um sistema simétrico?
2. Quantas chaves são necessárias trocar se existir um KDC (Key Distribution Center)?
3. Que vantagens tem a existência de um KDC quando comparado com um cenário onde esta entidade não existe?
4. Quantas chaves são necessárias se usar um esquema de chaves públicas? Diferencie estes esquemas em termos do número de chaves necessárias e a quantidade de chaves que coletivamente cada utilizador tem de guardar.

Exercício 3
Mostre que, no protocolo Kerberos, se as KEK forem comprometidas então um atacante pode recuperar todas as mensagens que foram trocadas.

Exercício 4
Estenda o protocolo Kerberos para que haja autenticação mútua entre as duas entidades. Apresente evidências de que a sua solução é segura.

Nível 1 – 1
Nível 2 – 2
Nível 3 – 3,4