Fundamentos de la Seguridad Informática

Primer Parcial

Criptografía

1. Explique cómo funciona un cifrado por única vez ("one time pad"). Indique su principal inconveniente.
   Explique qué similitudes y diferencias hay entre un cifrado stream y un cifrado por única vez. ¿Cómo compara la protección brindada por ambos métodos?

2.
   a) Indique un procedimiento (simplificado) para realizar una firma digital utilizando un algoritmo de clave pública.

   Para quien quiere verificar la firma realizada con el procedimiento anterior:
   b) Indique qué información debe poseer para poder verificarla
   c) Explique los cálculos que debe realizar. Justifique las garantías relacionadas con la seguridad que nos brindan.

IAA

3. Defina formalmente un Sistema de Autenticación. Dé un ejemplo de un sistema de este tipo y explíquelo.

4. Defina en forma precisa en qué consiste un Ataque de Usurpación de Identidad. Defina y explique los distintos tipos de Ataque de Diccionario.

Modelos

5. Describa formalmente los componentes del modelo Harrison, Ruzzo y Ullman (HRU). ¿Qué se entiende por un Sistema de Protección en el contexto de este modelo?

6. Explique lo más precisamente posible el concepto de Seguridad Multinivel. Describa un modelo que permite definir y validar políticas de seguridad de este tipo.

Bases de datos

7. ¿Cuál es el modelo de seguridad que define SQL? Justifique. Defina precisamente qué se entiende por privilegio en ese modelo.

Laboratorio

8. Laboratorio 1
   a) ¿Cuál es la principal diferencia, a nivel conceptual, en la gestión de las claves entre las infraestructuras criptográficas PGP y PKI?
      Explique detalladamente cada uno de los enfoques.
   b) ¿Cuáles son los posibles usos de las herramientas criptográficas GPG y OpenSSL?
      Indique por lo menos dos y explique.
   c) Indique si son verdaderas o falsas las siguientes afirmaciones, justificando:
      i. En el ataque Man-in-the-middle realizado, se obtuvo un mensaje encriptado que luego se tenía que procesar.
      ii. Como usuario pertenezco a un grupo que intercambia información en forma cifrada. Para pertenecer al grupo es requisito fundamental que mi certificado generado con OpenSSL esté firmado por al menos 3 miembros de dicho grupo.
      iii. A pesar del ataque visto en la práctica 3, MD5 se sigue usando pues sigue manteniendo la propiedad de resistencia débil a colisiones.
      iv. Un posible ataque a MD5 puede ser el siguiente: Un usuario genera un documento pdf que es enviado a una contraparte por una red insegura, antes genera el MD5 para enviárselo por otro canal a su contraparte. Un atacante mediante un ataque Man-in-the-middle captura el documento y genera uno con el mismo MD5 para retransmitirlo al destinatario y de esta forma engañarlo. Finalmente el atacante tiene éxito en su ataque.