Instituto Superior de Engenharia de Lisboa

Licenciatura/Mestrado em Engenharia Informática e de Computadores

Segurança Informática

First Assignment, Winter Semester 10/11

Due date: November 1st, 2010

---

1. Consider the existence of an attack on the SHA1 hash function, based on an efficient algorithm that, given x, obtains $x' \neq x$ such that $H(x) = H(x)$. What are the implications of this attack if this hash function is used in a digital signature scheme?

2. Consider the following scheme for the protection and non-repudiation of messages sent between A and B: m is the plain text message; (E_s, D_s, G_s) is a symmetric encryption scheme; (E_a, D_a, G_a) is an asymmetric encryption scheme; (S, V, G) is a digital signature scheme; K_e^B is the public key of B; K_s^A is the signature key of A.

   The protection of message m results in the following information sent to B:

   $$E_s(k_1)(m), S(K_s^A)(E_s(k_1)(m)), E_a(k_e^B)(k_1)$$

   where $k_1 = G_s()$.

   2.1. Describe the operations performed at the reception.

   2.2. Using this scheme, B can prove to other entities that A sent message m and not m'?

3. In the context of block based encryption schemes and the operation modes studied in class (i.e. ECB, CBC), consider a new operation mode defined by:

   - Let $x = x_1, \ldots, x_L$ be the division in blocks x_i of the clear text x.
   - Let $y_i = E(k)(x_i \oplus x_{i-1})$, with $i = 1, \ldots, L$, where E is the encryption operation, $\oplus$ is the bitwise exclusive OR and x_0 is the initial vector.
   - The cryptogram resulting from encrypting the plain text message x is $y = y_1, \ldots, y_L$.

   3.1. Define the decipher algorithm of this operation mode.

   3.2. What are the main problems of the ECB mode? The proposed operation mode solves these problems?

4. Consider the *Java Cryptography Architecture* (JCA).

   4.1. A PIN code (4 decimal digits) was encrypted with an asymmetric scheme, using an `Cipher` engine class instance. To initialize this instance, a `SecureRandom` object was used, whose method `nextBytes` always returns the same sequence of bytes. Describe a way to determine the PIN code, given the cryptogram.

   4.2. The `CipherOutputStream` class ensures the proper padding insertion in the produced cryptograms?

5. Consider a X.509 based public key infrastructure.

   5.1. Consider the scenario where a digital signature is produced with the signature key K_s, associated with the verification key K_v present in the certificate C. The certificate's subject name is A. Is the cryptographic verification of the signature sufficient to assure the verifier that the signature was produced by A?

   5.2. In the *Java Certification Path API*, why doesn't the `CertPath` class include the root certificate?

6. Consider the TLS protocol, presented in the course lectures.

   6.1. How is the integrity and confidentiality of messages exchanged between the client and server garanteed?

   6.2. In an usage scenario where clients are anonymous, why are the record protocol messages protected by a MAC scheme?

7. Consider the *Kerberos* protocol version presented in the course lectures.

   7.1. What is the need for the authenticator of A in messages sent by it to the TGS?

   7.2. Can the same ticket be used by the client to establish secure connections with two or more separate servers?

8. Develop, using the Java platform, an application for file authentication, based on the use of X.509 certificates. The application requirements are:

   - Signature File:
     - The signature operation receives the location of the file and produces a file with the resulting signature and its metadata.
     - The signature operation is also parameterized by a *key store* containing the private key to use in the signature process.
     - The metadata should include the certificate to be used to validate the signature, which is also found in the *key store*.
   - Signature verification:
     - The signature verification operation receives the location of the signed file and the file with the signature and the metadata.
     - The verification operation is also parameterized by: a directory containing the certificates of intermediate certification authorities, and a *key store* with the trust anchors used to validate the certificate chain.
     - The verification operation is performed only if the certificate is valid.

   Use the certificates and private keys found in the annex.

9. Using the techniques described by S. Vaudenay in the article *Security Flaws Induced by CBC Padding*, develop a Java application to decrypt the cryptograms present in the file `crypto`. The size of each cryptogram is 64 bits. The initial vector is the C_0 cryptogram. Use the `Cipher` static method, included in the `Oracle` class, as the oracle.

   Files `crypto` and `Oracle.class` are in the annex.

ISEL, 4 October 2010.