Topics in Information Security: Assignment

V Rohith

April 19, 2019

1. 7.7: Forged signature

   Considering the digital signature without hash function; where signing is done by:

   $$\text{Sign}(m) = E_{A.pr}(m)$$

   And signer sends m and Sign(m). Verification is done by checking

   $$m \stackrel{?}{=} E_{A.pu}(\text{sign}(m))$$

   A forged signature can be created in the following two scenarios. [using RSA]

   Scenario 1:

   - Attacker takes a σ and computes

     $$m = \sigma^e \bmod n$$
     $$\text{i.e, } m = E_{A.pu}(\sigma)$$

     and sends m, σ.
   - Verifier verifies that $m = \sigma^e \bmod n$ and concludes that m is signed by Alice.
   - **Note:** Here the message received - m, may not have any meaning. But attacker has succeeded in forging the signature.

   Scenario 2:

   - Attacker has two previously signed messages m_1 and m_2 with their signatures Sign(m_1) & Sign(m_2).
   - Now attacker can prepare a message

     $$m = m_1.m_2 \text{ and}$$
     $$\text{Sign}(m) = \text{Sign}(m_1).\text{Sign}(m_2)$$

     and sends m, Sign(m).

- The verifier checks that

$$\begin{aligned} m &= E_{A.pu}(\text{Sign}(m)) \text{ , since} \\ E_{A.pu} &= [\text{Sign}(m_1).\text{Sign}(m_2)]^e \bmod n \\ &= ({m_1}^d.{m_2}^d)^e \bmod n \\ &= (m_1 m_2)^{de} \bmod n \\ &= m_1 m_2 \bmod n \\ &= m \bmod n \end{aligned}$$

- Here the attacker has succeeded in forging the signature for a message m which is a product of two messages m_1, m_2. This is possible because of partial homomorphic nature of RSA.

2. 7.8: Number of messages required for Weak Collision Attack

If b is the number of bits of hash, there is a total possibility of $n = 2^b$ number of hash values.

Consider a message and its hash, consider we have prepared m number of identical messages.

$$\text{Prob(collision)} = \text{1 - Prob(No collision)}$$

$$= 1 - (\frac{n-1}{n})(\frac{n-1}{n})......(\frac{n-1}{n})$$

$$= 1 - (\frac{n-1}{n})^m$$

$$= 1 - (1 - \frac{1}{n})^m$$

Now using taylor series expansion of e^x, and ignoring second and higher order power of x,

$$e^{-\frac{1}{n}} = 1 - \frac{1}{n}$$

$$\text{Therefore, } P_c \approx 1 - e^{-\frac{m}{n}}$$

Rearranging the evaluation to get the number of messages m,

$$m \approx -n \ln(1-p) = n \ln(\frac{1}{1-p}) \tag{1}$$

Now for the attack to succeed with prob = 0.75, required number of messages is given by

$$\begin{aligned} m &\approx -2^b \ln(0.25) \\ m &\approx 1.3863(2^b) \end{aligned}$$

where b is the number of bits in the hash.