C2107 Tutorial 4 (PKI and SSL)

School of Computing, NUS

February 26, 2021

1. (**Birthday attack: selection from two sets**) Here is a variant of Birthday attacks. Some practical attacks can be analysed using this variant, e.g. DNS cache poisoning.

   Let $\mathcal{S}$ be a set of k distinct elements where each element is an n bits binary string. Now, let us independently and randomly select a set $\mathcal{T}$ of m n-bit binary strings. It can be shown that, the probability that $\mathcal{S}$ has non-empty intersection with $\mathcal{T}$ is more than

   $$1 - 2.7^{-km2^{-n}}$$

   Consider this scenario. There are $2^7 = 128$ students in the class. Each student is assigned a unique secret 16-bits id which is known by the student and the lecturer only. So, the chance of correctly guess the id of a particular student is 2^{-16}, which is quite small. One day, the lecture posted a multiple choice question during lecture and asked each student to write down the answer on a piece of paper together with the 16-bits id, and insert it into a box in the lecture hall.

   You know the correct answer and want to "share" with your classmates. You quickly write down the correct answer on 32 pieces of paper, each with a randomly chosen id, and covertly insert them into the box. What is the probability that at least one student benefit from your good deeds.

   How many pieces of paper do you need to submit, so that the probability is more than 0.5?

Solution

This variant differs from the original birthday attack in this way: In this variant, there are two sets of n-bit items, we select k from one set, m from the other set, and we ask whether there is a match between the two sets. In the original birthday attack, there is one set of n-bit items, we select k items, and ask whether there exist two items that match.

(a) Let $n = 16$, $k = 2^7$, and $m = 2^5$.
By applying the given formula, we have the probability ≈ 0.06 (which is low).

(b) We need to find m such that $1 - 2.7^{-km2^{-n}} = 0.5$.
We thus get $m \approx 362$.
Hence, you need to submit more than 362 pieces of paper.

(*Note*: There is also a quick approximation to find m simply by setting $k \cdot m = 2^n$, so that the probability becomes $1 - 2.7^{-1} = 0.63$.
We thus can find the approximate $m = 2^{16-7} = 2^9 = 512$.
This approximation is useful to have an approximate m.)

2. **(Certificate Structure)** A certificate issued by a CA contains at least these 4 pieces of important information (i) Name of an entity (ii) Public key (iii) Expiry data (iv) Signature s.

(a) For (ii), whose public key it is, the entity indicated in (i), or the CA?

(b) We know that the signature s is computed from a key k, together with a message m.

i. What is k? The entity's public key, the entity's private key, CA's public key or CA's private key?

ii. Which items in (i) to (iv) are to be included in m?

Note that the certificate also contains another important piece of information that indicates what type of functionality the public key can be used for, for example, verifying email address, or verifying domain name, etc.

Solution

(a) Entity indicated in (i)

(b) i. CA's private key.

ii. item (i), (ii), (iii).

3. What is a “self-signed certificate”?

Solution

The signature s is signed using the entity’s private key.

4. **(Certificate)** When Alice visited a website `www.c101.sg`, her browser displayed this prompt:

   “*Certificate’s signature is valid but is expired on 31 Dec 2020. I want to (1) accept the certificate and go ahead anyway (2) get me out of here.*”

   Alice chose option 1. What is the potential risk? (Describe a successful attack. Describe clearly the attack model/scenario. Do not give an attack that would succeed even if the certificate is not expired.)

Solution

Let the 4 pieces of information in certificate be D1, D2, D3, D4, i.e.

D1: Name, i.e. `www.c101.sg`

D2: Public key

D3: Valid range

D4: Signature

Since D4 is valid, this implies that the binding of the public key D2 to D1 is authentic during the time D3. Accepting this certificate is accepting an outdated, but valid information, e.g. sending a letter to an address that we are very sure valid 5 years ago. However, there are still possible scenarios of attack.

(a) The website `www.c101.sg` changed hand after D3. For e.g., a school just purchased the name for a module C101 on 1 Feb 2020. The previous owner has a valid but outdated certificate, and he used this against Alice.

(b) The website has some disputes with an ex-employee who knows the private key of D2. Since the certificate already expired, the website doesn't need to revoke the certificate. Now, this ex-employee used this against Alice. This can be viewed as an insider's attack.

The next scenario (c) is realistic. But if the question states clearly that the crypto parameters are the same, it will not be applicable.

(c) The outdated certificate use SHA1 and thus the D4 can be forged.

This scenario (d) is not accepted as an answer:

(d) The attacker has more time in forging the signature.

5. **(MAC)** It is tempting to design a mac using encryption. Given a message m and key k, the mac is $\text{Enc}_k(H(m))$ where $H(\cdot)$ is a collision resistant hash, and $\text{Enc}_k(\cdot)$ is some symmetric key encryption. In addition, $\text{Enc}_k(\cdot)$ is believed to be secure with respect to confidentiality.

Explain why it might not be a secure mac.
(Hint: AES Counter mode is believed to be secure with respect to confidentiality. Optional Remark: a well accepted notion of security (w.r.t. confidentiality) is Indistinguishability under Chosen-Plaintext-Attack.)

Solution

Let us assume that $\mathrm{Enc}_k(\cdot)$ is AES Counter mode, that is, it is a stream cipher.
Suppose the adversary has a valid pair of message m_0 and its mac t_0. Now, the adversary chooses a m_1 such that $m_1 \neq m_0$. Since t_0 is the ciphertext of AES Counter mode, it is of the form $t_0 = v \| c$ where v is the IV and c is the xor'ed of m_0 with the pseudorandom sequence. Let $t_1 = v \| (c \oplus H(m_1))$. Note that t_1 is a valid mac for m_1. So the adversary has successfully forged a mac.

Remark: For certain choice of encryption schemes, the above hash-and-encrypt can give a secure mac. What we have shown above is that, in general, an encryption scheme, which is secure w.r.t. confidentiality, does not guarantee to give a secure mac. In some sense, confidentiality does not give integrity.

6. Visit `https://luminus.nus.edu.sg` using your favourite browser. Find the certificate of the website and the 4 pieces of information mentioned in Question 3. Very often, we say that the RSA's public key consists of the modulo n and an encryption exponent e that is randomly chosen. LumiNUS happens to employ RSA public key. What is the LumiNUS's value of e? In practice, e is seldom randomly chosen and is a fixed small value (no known vulnerability for that). What is the advantage of having a small value instead of a randomly chosen one?

Solution

e is 65537.
If e is small, the computation to be carried out by the public (in this case, it is the signature verification, which essentially is to compute exponentiation to e) would be lighter. The smallest possible is $e = 3$. However, when e is too small, there is a vulnerability under a very special scenario. Hence, NIST recommends e to be greater than 65536.

7. Find out the list of certificates installed in your favoured OS/browser.