C2107 Tutorial 4 (PKI and SSL)

School of Computing, NUS

February 24, 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.

   $1 - 2.7^{-128(32)2^{-17}}$

   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.

   $m > \frac{\log 0.5}{-128(2^{-17})\log(2.7)}$

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

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.

3. What is a "self-signed certificate"?

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.)

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

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?

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