CS2107 Tutorial 4 (PKI, SSL and Birthday Attack Variant)

School of Computing, NUS

16–20 September 2019

1. (*Certificate structure:*) Recall that a certificate issued by a CA contains at least the following four pieces of important information:
   (i) Name of an entity; (ii) Public key; (iii) Validity period; and (iv) Signature.

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

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

      i. Whose key k is it: the entity's public key, the entity's private key, CA's public key, or CA's private key?

      ii. Which pieces of information in (i)–(iv) are to be included in the message m?

2. (*Certificate type:*) What is a "self-signed certificate"? Who typically uses one?

3. (*Certificate usage:*) Find out the list of certificates installed in your favoured OS, browser, and also smart phone. Did you found anything suspicious?

4. (*Proxy re-encryption CA system:*) A school has a local area network that is connected to the Internet via a gateway. All incoming and outgoing traffic to the Internet therefore must go through the gateway. As part of their responsibilities to the students' parents, the school wants to inspect all the network communication made by the students, and thus have installed a monitoring agent M at the gateway.

   (a) Suppose Alice is in the school. Alice often visits the webpage:

   `https://www.happytooth.com`

   to make her dental appointments. Can the monitor M find out Alice's appointment details by inspecting the traffic. Why?
   (*Hint:* Recall that https works "on-top" of SSL/TLS, which is described in the lecture notes.)

   (b) The school insists that all network traffic via the gateway must be inspected. Hence, whenever the monitor M spots "encrypted" communication, it will drop them. Explain why this solution is not desired.

   (c) The students, in particular Alice, violently protest. As a compromise, the school allows the students to visit webpages using https, but with the condition that the monitor is able to decrypt and inspect the communication. The students are happy with this arrangement. The school approaches you for a solution. Do you have something for them? How about the idea of making students' browsers forward to M any session keys that they share/establish with external sites? Is it a feasible and good solution?

(d) You search the Web, and have a better idea. The solution is as follows:

i. All students must accept a self-signed certificate with the entity name `SchoolCA` and its public key k_e. This certificate also states that `SchoolCA` can issue certificate, that is, it is a CA. The school and the monitor M know the private key k_d of k_e.

ii. Now, whenever a student, say Alice, wants to visit a https site, say `https://www.happytooth.com`, the monitor can carry out "proxy-re-encryption" to decrypt the communications, inspect, and then re-encrypt them.

Explain how the step (ii) above is to be carried out. You can use the following step-by-step guide to explain the process.

(a) Suppose Alice wants to visit `https://www.happytooth.com`. To make it easy, let's call the website simply *Bob* in this description.

(b) The monitor M sits in the middle of Alice and Bob. Hence M can be a *man-in-the-middle*. (*Note*: In fact, M is a very powerful man-in-the-middle since it knows the `SchoolCA`'s private key k_d.)

(c) First, Alice has to carry out a unilateral authentication with Bob as mentioned in the lecture notes. However, now M pretends to be Bob, and carries out the authentication as follows.

(d) To get authenticated by Alice, M needs to show that it knows the private key of a public key associated with the identity _____. M can achieve this by issuing a certificate with the content _____, and uses the certificate in the authentication process with Alice.

(e) Alice will accept the information listed in the certificate issued by M, because _____.

(f) After a successful authentication, M and Alice establish a session key pair k_1, t_1 (see lecture notes). All communication will be encrypted using _____ and authenticated using _____.

(g) M then performs a unilateral authentication with Bob. After a successful authentication, M and Bob establish another session key pair k_2, t_2. All communication between M and Bob will be encrypted using _____ and authenticated using _____.

(h) Now, when Alice makes her dental appointment, the message is to be encrypted using _____ and sent to M. M decrypts it using _____, inspects it, and then re-encrypts it using _____, and finally forward it to Bob.

(i) Likewise, for the message from Bob to Alice are processed in a similar way. Bob's message is to be encrypted using _____ and sent to M. M decrypts it using _____, inspects it, and then re-encrypts it using _____, and finally forward it to Alice.

5. (*A variant of birthday attacks:*) Here is a variant of Birthday attacks:

   Let $\mathcal{S}$ be a set of k distinct elements, where each element is a n-bit binary string. Now, let us independently and randomly select m n-bit binary strings. It can be shown that, the probability that at least one of the randomly chosen strings is in $\mathcal{S}$ is (more than):

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

   (*Note*: Notice that the set $\mathcal{S}$ and the set of the generated m strings are different!)

   Now, consider this scenario. There are $2^7 = 128$ students in the class. Each student is assigned a secret 16-bit ID, which is known only by the student and the lecturer. The probability of correctly guessing the ID of a particular student is thus 2^{-16}, which is very small. One day, the lecturer posted a multiple choice question during the lecture, and asked each student to write down the answer on a piece of paper together with his/her 16-bit ID, and insert it into a box in the lecture hall.

   Suppose you know the correct answer, and want to generously share it 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.

   (a) What is the probability that at least one student benefits from your attempted good deed?

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

   (Remark: Some attacks are similar to the above scenario, particularly "DNS cache poisoning" attack.)

— End of Tutorial —