CS2107 Tutorial 5 (PKI, TLS/SSL, and Birthday Attack Variant)

School of Computing, NUS

27 September – 1 October 2021

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?

   Solution

   (a) The public key in (ii) belongs to the entity indicated in (i).

   (b) i. The key k is CA's private key.

      ii. The message m includes items (i)–(iii).

      (*Note:* Notice again that signature operation is not the same as *encryption* with private key. While RSA operates in this way, there are many other public-key signature schemes that do not, such as ElGamal signature scheme and Digital Signature Algorithm (DSA).

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

   Solution

   A "self-signed certificate" is a certificate that is signed by the stated entity's private key.
   It is used by a root CA. It is also quite commonly used by developers during the early stage of software development period when a valid certificate of a relevant host is not available yet.

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

Solution

Please google to find out how you can view the lists of installed certificates in your systems and browsers.

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 TLS/SSL, which is described in the lecture notes.)

   Solution

   No. Because HTTPS employs TSL/SSL to establish a secure channel between two communicating parties, where all the communicated messages are encrypted.

   (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.

   Solution

   The students will be unhappy since they can't perform many important online transactions with various websites that employ the widely-used HTTPS protocol.

   (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?

Solution

The proposed solution will be very difficult to implement since it requires a browser change. This requirement poses a serious problem since the school needs to make the required modifications on various types of popular Web browsers on different OS platforms, and their numerous available versions. Also, browsers do get updated very frequently by their developers, including for security reasons. The solution is therefore not feasible.

(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.

Solution

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

ii. 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 can inspect HTTPS traffic too as explained below. This is since M knows the `SchoolCA`'s private key k_d, thus allowing it to issue and sign any certificate that will be accepted by the students.)

iii. 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.

(Note: As mentioned in the lecture notes, HTTPS is used to perform a unilateral authentication. The outcome of the employed TLS/SSL handshake protocol is to derive session keys for encrypting and protecting the authenticity of subsequent communication.)

iv. To get authenticated by Alice, M needs to show that it knows the private key of a public key associated with the identity **Bob**. M can achieve this by issuing a certificate with the content **(i) Bob; (ii)** k_e**; (iii); Validity period; (iv) Signature done using** k_d **of the `SchoolCA`'s certificate**, and uses the certificate in the authentication process with Alice.

v. Alice will accept the information listed in the certificate issued by M, because **Alice has accepted the `SchoolCA`'s certificate**.

vi. 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 $\boldsymbol{k_1}$ and authenticated using $\boldsymbol{t_1}$.

vii. 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 $\boldsymbol{k_2}$ and authenticated using $\boldsymbol{t_2}$.

viii. Now, when Alice makes her dental appointment, the message is to be encrypted using $\boldsymbol{k_1}$ and sent to M. M decrypts it using $\boldsymbol{k_1}$, inspects it, and then re-encrypts it using $\boldsymbol{k_2}$, and finally forward it to Bob.

ix. Likewise, for the message from Bob to Alice are processed in a similar way. Bob's message is to be encrypted using $\boldsymbol{k_2}$ and sent to M. M decrypts it using $\boldsymbol{k_2}$, inspects it, and then re-encrypts it using $\boldsymbol{k_1}$, 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.)

Solution

(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 technique is useful in case you don't have a calculator with you, or you just want to have an approximate m.)

— End of Tutorial —