UNIVERSITY OF EDINBURGH

COLLEGE OF SCIENCE AND ENGINEERING

SCHOOL OF INFORMATICS

INFR09025 COMPUTER SECURITY

Tuesday 6 th May 2014

14:30 to 16:30

INSTRUCTIONS TO CANDIDATES

Answer any TWO questions.

All questions carry equal weight.

CALCULATORS MAY NOT BE USED IN THIS EXAMINATION

Year 3 Courses

Convener: S. Viglas
External Examiners: A. Cohn, T. Field

THIS EXAMINATION WILL BE MARKED ANONYMOUSLY

1. We consider the following identification protocol. Let G be a cyclic group of prime order q. Let g be a generator of G. Let also $x \in \mathbb{Z}_q$ be chosen at random, and let $sk := x$ be the prover's secret key. Finally, let $vk := g^x$ be the corresponding public verification key. Now, the protocol works as follows:

   (α) the prover picks a random $r \in \mathbb{Z}_q$ and sends $R := g^r$ to the verifier;

   (β) the verifier picks a random challenge $c \in \{1, \ldots, B\}$ (for some fixed integer B) and sends c to the prover;

   (γ) the prover computes $z := x \cdot c + r \pmod{q}$ and sends z to the verifier;

   (δ) the verifier outputs "yes" if and only if $g^z = (vk)^c \cdot R$.

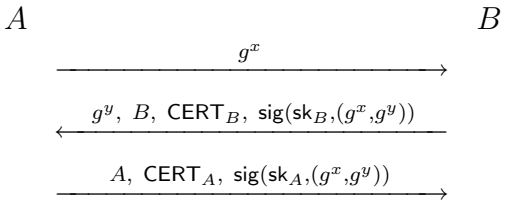
   The purpose of this protocol is for the prover to prove to the verifier that he is indeed the owner of the secret key x corresponding to the public key vk.

   (a) Show that the reply of an honest prover (following the protocol) to the verifier's challenge will always be accepted by the verifier (*i.e.* the verifier will output "yes"). [*5 marks*]

   (b) Suppose steps (α) and (β) of the protocol are swapped, *i.e.* step (β) takes place before step (α). Show that, in that case, an attacker who knows vk, but does not know the corresponding secret x, can cause the verifier to accept his answer to the verifier's challenge. [*10 marks*]

   (c) Suppose the prover accidentally responds to two challenges c and c' without changing R. Show that the verifier can use (vk, R, c, c', z, z') to recover x. [*10 marks*]

2. In class, we saw the Diffie-Hellman protocol, which is a two-party key establishment protocol secure against passive attackers. However, as we saw, the Diffie-Hellman protocol is insecure against active attackers. Indeed, a malicious agent can mount a man-in-the-middle attack to learn a key not intended for him. This attack is possible because there is no mechanism to authenticate the two parties to one another. We consider the following extension of the Diffie-Hellman protocol to thwart this attack. We assume that the parties A and B have a private signing key sk_A and sk_B respectively, and a certificate on the corresponding public key CERT_A and CERT_B respectively.



The result is a shared secret $K_{AB} = g^{xy}$ from which the parties derive a session-key. You can consider the certificate CERT_X to be a signature issued by a trusted third party on X's public key, *i.e.* $\mathsf{CERT}_X = \mathsf{sign}(\mathsf{sk}_{TTP}, (X, \mathsf{pb}_X))$.

(a) Explain the purpose of the signatures in the protocol above. How does it defend against the attack discussed in class? [*5 marks*]

(b) Show that an active man-in-the-middle attack is still possible. More precisely, show that malicious Eve can cause:

- A to think that she is communicating securely with B (as required),
- B to think he is communicating securely with Eve.

In other words, B is fooled into thinking that the subsequent encrypted messages he is receiving (from A) are coming from Eve. Note that Eve cannot eavesdrop on the resulting encrypted channel.
Hint: Eve replaces the third message. You may assume that Eve also has a certificate, CERT_E, on her public signature verification key sk_E. [*7 marks*]

(c) Describe how Eve can use the attack from Question 2 to steal money from A. For example, suppose A gives expert advice in a private chat room run by B, and that she gets paid for that. [*3 marks*]

(d) Propose a way to fix the protocol to defend against the attack from Question 2. Explain why your fix prevents this attack. [*10 marks*]

3. An international media distribution company *YourFlix* is establishing a web site in order to distribute downloaded movies. At registration, each user u_i is given a distinct symmetric key K_i stored in a secure keystore that is used to access their movies at their computers. A copy of each key is also securely held by the distributor.

   YourFlix has offered to pay you, based upon your security background, for advice in three areas.

   (a) They have developed three options for protecting the confidentiality of a movie M, which will be several gigabytes in size.

   - Option 1. The movie M is encrypted individually for each user u_i as $E_{K_i}(M)$.
   - Option 2. The movie is encrypted with a separate symmetric key K as $E_K(M)$, and K is encrypted for each u_i as $E_{K_i}(K)$.
   - Option 3. Similar to the previous option, except that the symmetric key K is encrypted for each user u_i as $E_{K_i}(K) = K \oplus K_i$.

   Discuss and compare the options in terms of their security, as well as feasibility and cost to implement each. Which method is preferable? Are there any additional confidentiality issues that they should also address? [*8 marks*]

   (b) YourFlix recognize a need for *network security* protections for their distribution network, but are unsure of the methods they should use. Provide some advice for them regarding *firewalls*, *intrusion detection systems*, and *honeypots*, by defining each, reviewing the different types, and discussing their advantages and disadvantages. [*8 marks*]

   (c) YourFlix are particularly concerned about *software security*, and ask for your advice. Describe three common programming failures that can lead to a security attack that might be relevant for a movie distribution network, and suggest a possible countermeasure for each. [*9 marks*]