UNIVERSITY OF BIRMINGHAM

School of Computer Science

MSc Cyber Security

06 28214

Designing Secure Systems

Summer May/June Examinations 2016

Time allowed: 1 hour 30 minutes

[Answer ALL Questions]

No Calculator

[Answer ALL Questions]

1. (a) Explain three well-known principles of secure design. [15%]

(b) A company wants your help in designing a WiFi-enabled central heating controller; the idea is that customers can control their central heating from a web page or app. For each of the principles you identified in (a), explain

- a possible attack on the WiFi-enabled heating controller;

- a possible mitigation of the attack based on applying the principle.

Your answer should be concise (it is recommended to use about 30 words for each attack and mitigation). It is permitted to use the same attack when discussing different principles. [18%]

2. A bank offers an online banking service. When users register, they are asked to create a 10 character password. Later, when they login, the server randomly chooses three positions in the range {1,2,...,10} and asks the user to cite the characters of their password at those positions. For example, the server might choose the positions 1, 3 and 7, and therefore ask the customer to cite the first, third and seventh characters from their password.

The bank consults you on how it should store the user's passwords, and is considering the following options. Let u be a user id, and p the user password, and let H be a hash function (such as SHA2).

(a) Store u and p in the database. [8%]

(b) Store u and H(p,s) and s in the database. Here, s is a per-user randomly-chosen salt value. [8%]

(c) Store u and H(p1,s1), H(p2,s2), …, H(p10,s10) in the database. Here, pi is the ith character of the password, and si is a per-user and per-position randomly-chosen salt value, for each position i in {1,...,10}. [8%]

For each of the schemes above, explain in what way it is unsatisfactory from a functional or security point of view.

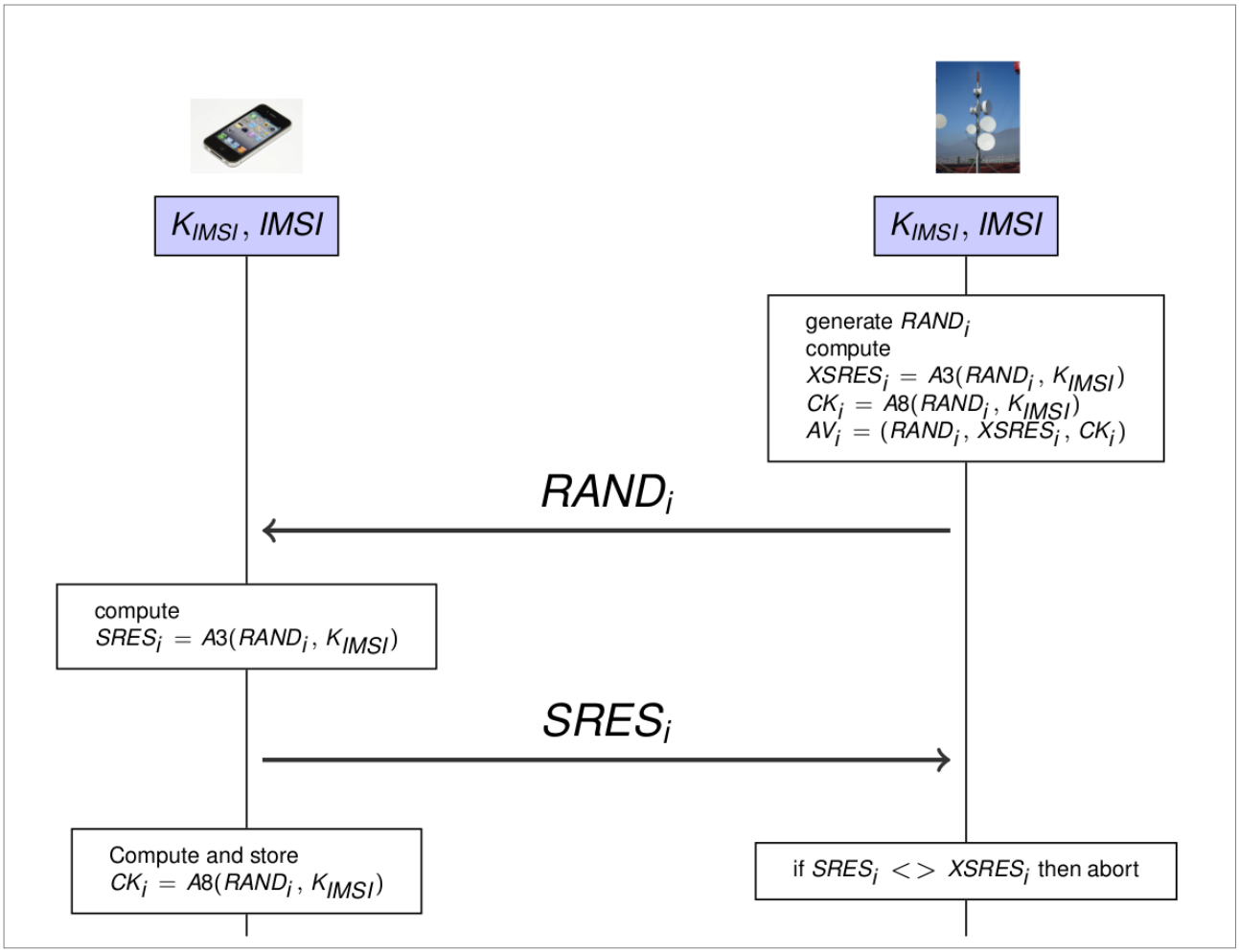
(d) Explain a way of storing the user passwords that you consider satisfactory. [9%]

3. (a) Explain the concepts of *International Mobile Subscriber Identity* (IMSI) and *Temporary Mobile Subscriber Identity* (TMSI) in mobile telephony. [8%]

The figure below shows the authentication protocol used in 2G mobile telephony. K_{IMSI} is a pre-shared key between the mobile handset (shown on the left of the diagram) and the network (shown on the right).

(b) Briefly explain how the mobile handset authenticates itself to the network, as shown in the diagram. [8%]

(c) Does the network authenticate itself to the mobile handset? Explain your answer. [9%]



(d) The authentication protocol in 3G telephony improves on the 2G one shown, because in 3G the network authenticates itself to the mobile handset. Briefly explain how that is done. [9%]