MANCHESTER 1824

The University of Manchester

COMP61421 - Cyber Security

Assignment 2 - A Drink Vending Machine

Maximum marks available in this coursework	50
Weighting of this coursework towards the unit overall mark (%)	50%
Learning outcomes being Assessed	Stated in the course unit specification
The coursework setter	Dr Ning Zhang
Handout date	7th Dec 2020
Handin date	4:00pm, 22nd January 2021 (Please submit your work via the Blackboard facility)

The Problem

An advanced drinks vending machine allows a mobile user to pay for a drink using a mobile phone billing account based on his/her fingerprint. The user is assumed to have data related to one of his/her fingerprints registered with a server operated by the service provider that manages the user's billing account. To purchase a drink, the mobile user uses his/her mobile phone to dial the number associated with the vending machine, and the machine then displays a request for the selection of a drink and provision of data related to the user's fingerprint. Having received the user's valid drink selection and user's fingerprint related data, the vending machine uses the fingerprint related data to request the server of the user's service provider to pay for the drink selected. Here assume that the vending machine can obtain the user's phone number and identify the server of his/her service provider based on the number.

Upon receipt of the vending machine's payment request, the server checks that it has a billing account associated with the fingerprint data received and the amount of money in the account is sufficient to pay for the drink. The server grants the payment by debiting the user's billing account and crediting the designated account of the vending machine, only if the checking is positive, and informs the vending machine of its decision. If the server grants the payment, the vending machine delivers a selected drink. Otherwise, the vending machine terminates the purchase and informs the user by a displayed message.

only consider the situation that customer's phone is ordinary which don't have a built-in fingerprint scanner

The drinks vending machine is mainly designed for a mobile user using an advanced mobile phone with a built-in fingerprint scanner. However, sometimes the mobile user can only get hold of an ordinary mobile phone with no built-in fingerprint scanner. In this case, the user is allowed to download his/her fingerprint related data from the server of the user's service provider. This coursework *only* considers the latter case.

It is assumed that:

- Each user's mobile phone offers a AES-based symmetric cryptosystem including a secure hash function;
- The user has a password registered with the server of his/her service provider but does not share any extra AES key with the server;
- The user does not share any AES key with the vending machine;
- The user's mobile phone cannot run any asymmetric cryptosystems such as RSA and DH (Diffie-Hellman);
- For the sake of cost-saving, the use of Kerberos has been ruled out.

The Questions

You are required to perform the following tasks (you can make necessary assumptions):

1. Secure downloading of a mobile user's fingerprint related data. This includes:
   (a) Design and explain (with diagrammatical illustration) a protocol to allow the mobile user to securely download his/her fingerprint related data from the server of the user's service provider to his/her mobile phone.

Note that the design of this protocol must meet the following requirements:

(i) The server transfers the fingerprint related data to the mobile user only when the server is convinced that the user is the legitimate owner of the fingerprint related data and that the request is indeed from the claimed user.

(ii) The confidentiality of the fingerprint related data transferred from the server to the user must be protected.

(iii) Measures should be taken to reduce the risk of Denial of Service (DoS) attacks on the server.

(b) Analyse the designed protocol to justify how the protocol satisfies the above requirements 1 (a) (i), (ii) and (iii).

2. Authorised purchase of a drink by a mobile user. This includes:

(a) Design and explain a protocol (with diagrammatical illustration) to allow the mobile user to purchase a drink based on his/her fingerprint related data already downloaded from the server of the user's service provider to his/her mobile phone.

Note that the design of this protocol can omit the details of the drink purchase (e.g. the drink price and account details of the drink vending machine), and that the design must meet the following requirements:

(i) The mobile user authorises the drink purchase using his/her fingerprint related data, the drink vending machine receives the authorisation but cannot obtain any information on the user's fingerprint data, and the service provider's server can verify the authenticity of the user's authorisation and the vending machine's payment request.

(ii) The drink purchase authorisation of the mobile user cannot be re-used for deceptive charging by the vending machine if it misbehaves, the authenticity of the response by the server to the payment request should be assured and the mobile user can obtain an authentic e-receipt for the purchase.

(b) Analyse the designed protocol to justify how the protocol satisfies the above requirements 2 (a) (i) and (ii).

(c) Analyse the computational and communication costs of your designed protocol.

What you should hand in

Written report on results of all the tasks specified in the above section "The Questions", in which all descriptions and diagrams must be word-processed. For full marks your answer should be complete (all the design details should be provided, and design decisions justified), concise as well as accurate.

Guidelines/Length

This is an **individual** coursework, so it must be completed **independently**.

This coursework should be carried out with reference to relevant textbooks and published articles. The length of the report should not exceed four A4 sides (i.e. approximately no more than 2000 words).

Assessment

Task	Assessment Criteria	Raw marks for each problem component
	Clear statement of assumptions made	3
1	Correct protocol design, clear explanation, and convincing analysis against the specified requirements	14
2	Correct protocol design, clear explanation, and convincing analysis against the specified requirements	28

	Report clarity and quality (clear justifications, protocol efficiency considerations, conciseness and accuracy, evidence of research)	5

Additional notes:
Submissions: This is the **2nd** of **three** assessed submissions for this unit.
Late Submissions: Extensions will only be granted as a result of formally processed Mitigating Circumstances (please contact SSO, the Student Support Office, with regard to mitigation circumstances). Marks for late submissions will be reduced in line with the following university policy (http://documents.manchester.ac.uk/display.aspx?DocID=24561).
Support: Support is available in the afternoon of Day 5 of this module teaching period. Additionally, questions can be posted on the Blackboard forum.

End of the Coursework