### A Drinking Vending Machine

Huanjie Guo ID:10655496

**1. Secure downloading of a mobile user’s fingerprint related data.**

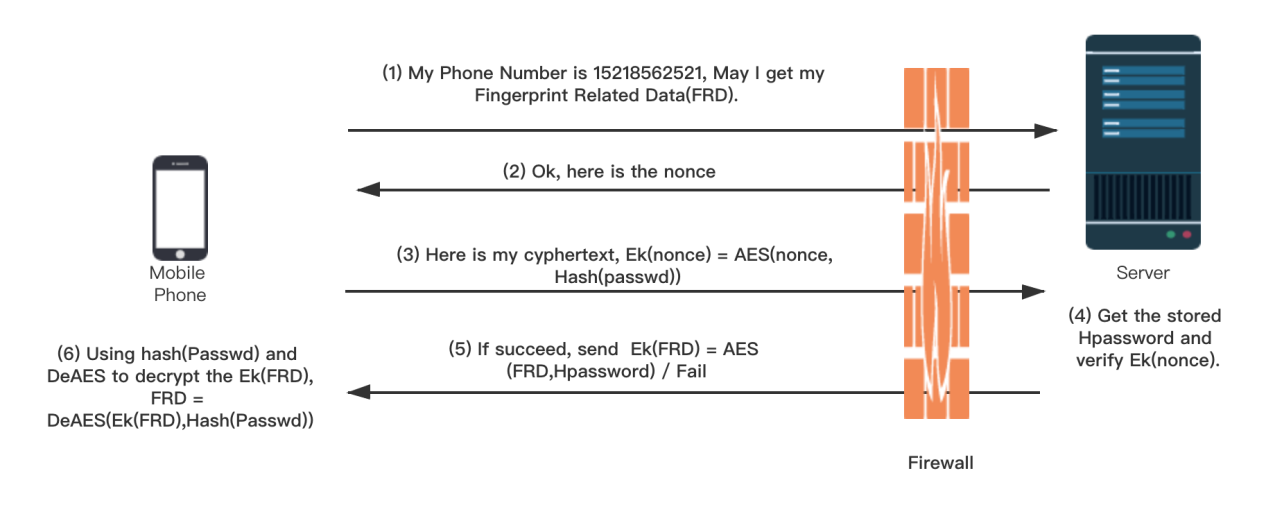


Image 1 How to tranfer FRD.

**(a) Design and explain.**

The protocol to secure downloading of a mobile user’s fingerprint related data has 6 steps.

1) The mobile phone sends a request to the server to ask to get the finger related data of the specific phone number.

2) Server receives the request and sends a nonce(N) to the mobile phone, nonce = timestamp(length of 13)+'\_'+random\_digits(length of 10), then use nonceMap.put(phone,nonce) to put this nonce into its cache.

3) Mobile phone receives the nonce(N), then apply the Hash function to get Hpasswd, which is produced by Hash(Passwd)[1]. After that, the mobile phone uses the AES[2] algorithm with the Hpasswd as a key to encrypt the nonce, then get Ek(nonce) = AES(nonce, Hpasswd) and return Ek to the server.

4) Server receives cyphertext Ek1, then it goes to its cache to get the nonce by using nonceMap.get(phone). As mentioned in step 2, the nonce is the combination of a timestamp and random number, so the server uses the split function to get the record\_timestamp from nonce. After that, the server calculates the time interval between current\_timestamp and record\_timestamp, and if it is larger than 5 seconds, the authentification is failed. If it is within 5s, the server gets the user's Hpasswd from the database, uses AES to get Ek2 = AES( nonce, Hpasswd). If Ek1 = Ek2, the authentication is succeeded. Otherwise, it fails.

5) If step 4 is succeeded, the server use AES to encrypt fingerprint related data with the user's Hpassword as a key, get Ek(FRD) = AES(FRD, Hpassword), then send it to the mobile phone. If the server cannot authenticate the identity of users in step 4, it returns messages to notify users.

6) Mobile phone receive cyphertext Ek(FRD), then it uses AES to get user's fingerprint related data, FRD = DeAES( Ek(FRD),Hash(passwd)).

**(b) Analyse the designed protocol.**

**(i) How does this protocol make sure that 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?**

The server checks the identity in steps 2, 3, and 4. Only when the user has the correct passwd of the account, it can give the correct Ek(nonce) to the server, so the user is the legitimate owner of FRD. If the Ek(nonce) is watched by eves, it will be invalid soon within 5 seconds because in step 2 the server put timestamp into nonce.

**(ii) How does this protocol make sure that the confidentiality of the fingerprint related data transferred from the server to the user must be protected?**

In step 5, we use AES to encrypt the FRD, and only when the receiver has the password of the account, he can get the FRD.

**(iii) What measures are taken to reduce the risk of Denial of Service (DoS) attacks on the server?**

(1) Add proxies to the firewall to filter out ICMP packets and spoofing packets.

(2) Decrease TCP connection timeout[3] and limit the number of new connections from an IP per timeframe. At the same time, block some IPs if it is continually trying to establish TCP connections.

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

**(1) Computational Costs**

|  |  |  |  |
| --- | --- | --- | --- |
| Function | times | Speed | Step |
| Sha256 | 2 | fast | 3,4 |
| AES-Encode-256 | 2 | fast | 3,5 |
| AES-Decode-256 | 2 | fast | 4,6 |

Thanks to the boosting performance of the CPU, the computational cost of this protocol is totally acceptable.

**(2) Communication Costs**

In this protocol, there are four communications before the mobile phone gets its fingerprint related data. For the sake of security, it is acceptable.

**2. Authorised purchase of a drink by a mobile user.**



Image 2 Authorise purchase

**(a) Design and explain.**

The protocol to authorize the purchase of a drink by a mobile user has 7 steps.

1) The mobile user dial the machine associated number to connect to the vending machine.

2) The drink vending machine sends the order detail to the mobile phone and asks the user to do the encryption.

3）Mobile user uses his fingerprint related data (FRD) as the key to do the AES process and get the

Ek(Ord),Ek(Ord)= AES (Ord,FRD), then sends it to the drink vending machine.

4) The drink vending machine receives Ek(Ord).

(1)The vending machine produces payment request PReq = (Ek(Ord),phone).

(2)The vending machine uses the key shared with the server to encrypt the PReq, Ek1(PReq) = AES(PReq, key).

(3) Send Ek1(PReq) to the server.

5) The server receives Ek1(PReq). Then do the process as follow:

(1) Use the key shared with the vending machine to decrypt Ek1(PReq), PReq = DeAES(Ek1(PReq),key). Here PReq = (Ek(Ord),phone).

(2) Use the user's phone number to search the user's FRD from the database.

(3) Use FRD to decrypt Ek(Ord), Ord = DeAES(Ek(Ord),FRD). If the server cannot decrypt it, the validation fails.

(4) Interval = currentTimestamp - Ord.createTime. If Interval is larger than 5 seconds, the validation fails.

(5) Search Ord.id from the database. If it exists, the validation fails.

(6) Here, the validation passes. The server tries to reduce the balance from the user's wallet,then record the Ord.id in the database.

6) The server uses the key shared with the drink vending machine to encrypt the result of the payment and the E-receipt, then send it to the drink vending machine.

7) The drink vending machine uses the key to decrypt the cyphertext and get the payment result and the E-receipt. If the result shows success, the vending machine gives users the drink ordered and prints the receipt. Otherwise, it terminates the purchase and informs the user by a displayed message.

**(b) Analyse the designed protocol.**

**(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**.

The vending machine sends the order to the mobile phone in step 2, then the mobile user AES with fingerprint related data to encrypt the order then send it to the vending machine in step 3. In this way, the vending machine cannot obtain the user's FRD.

**The service provider’s server can verify the authenticity of the user’s authorisation**

The server use user's phone to search his FRD from the database then uses it as the key to decrypt the Ek(Ord) in step 5 and get the Ord. So, the server can verify it.

**The service provider’s server can verify the authenticity of the vending machine’s payment request.**

We assume that the server and the vending machine share the same key. The vending machine encrypts the payment request Ek1(PReq) = AES(PReq, key) and sends it to the server in step 4. The server decrypts it by PReq = DeAES(Ek1(PReq), key) in step 5. In this way, the server can verify the authenticity of the 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.**

In step 5, the server can check if the order is produced within 5 seconds. Besides, the order information such as Ord.id was recorded in the database, so the purchase authorization cannot be reused anymore.

**The authenticity of the response by the server to the payment request should be assured.**

We assure the server and the vending machine share a key. In step 6, the server encrypts the response of the payment result, Ek(PRes) = AES(PRes, key), and in step7, the vending machine decrypts it and gets the payment result, PRes = DeAES(Ek(PRes), key). In this way, the authenticity of the response by the server can be assured.

**The mobile user can obtain an authentic e-receipt for the purchase.**

In step 6, if the payment result shows success, the server use user's FRD as the key to encrypt the E-receipt and the payment result then send it to the vending machine. In step 7, the vending machine receive it and decrypt it to get the payment result and E-receipt.

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

**(1) Computational Costs**

|  |  |  |  |
| --- | --- | --- | --- |
| Function | times | Speed | Step |
| AES-Encode-256 | 3 | fast | 3,4,6 |
| AES-Decode-256 | 3 | fast | 5(twice),7 |

The computational cost of this protocol is totally acceptable.

**(2) Communication Costs**

In this protocol, there are 5 communications before the user gets his drink from the vending machine. For the sake of security, it is acceptable.

**Reference**

1. Carter J L , Wegman M N . Universal classes of hash functions[J]. Journal of Computer and System Sciences, 1977, 18(2):143-154.
2. Daemen J , Rijmen V , Leuven K U . AES Proposal: Rijndael[J]. 1998.
3. G. Carl, G. Kesidis, R. R. Brooks and Suresh Rai, "Denial-of-service attack-detection techniques," in IEEE Internet Computing, vol. 10, no. 1, pp. 82-89, Jan.-Feb. 2006, doi: 10.1109/MIC.2006.5.