Question 3: How secure is eduroam

a) KoreK, PTW and WPA Dictionary attack

First we need some information about eduroam:

- security: WPA2 Enterprise / AES
- EAP Type secured EAP (PEAP, EAP-TTLS, EAP-TLS, EAP-FAST)
- uses certificates

Sources:

- https://www.tubit.tu-berlin.de/wlan/
- https://wiki.geant.org/display/H2eduroam/eduroam+in+a+nutshell

KoreK and PTW are attacks that only work on WEP and a Dictionary attack does not work on account based authentification.

There is no practical attack on WPA Enterprise with this configurations known to us, but there are some other approaches.

b) Other methods for attacking eduroam

In WPA2 Enterprise we do not authenticate directly against the AP, but the request is forwarded to a RADIUS server that does not only check the for the passphrase but requires account based authentification.

Possible attack methods for eduroam and other WPA/WPA2-Enterprise networks:

1. ***Spoofing an eduroam Access Point***: Setting up a fake Access Point, which mimics true eduroam APs, with own RADIUS server that logs username and tokens. Then force associated user to deauthenticate and connect to the faked eduroam AP and hope they accept the untrusted certificate. After that we can get the credentials hashes of challenge/response protocol (from our malicious RADIUS server logs) and we can crack them with John the Ripper or Hashcat. Also in at university we would pick a campus where less technical versed victims roam but internet access is essential

2. ***Phishing the credentials via email.***

3. ***Exploiting the OpenSSL heartbleed vulnerability*** if there is a RADIUS server, that hasn’t patched it yet (low probability). This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the transfer of user credentials from the user’s device to their home institutions RADIUS server. The home RADIUS server X.509 credentials are also used to authenticate the home RADIUS server i.e. to ensure the user is delivering credentials to their home RADIUS server.
   If an intruder is able to create an eduroam hotspot (e.g. using an eduroam in a box setup with a rogue Access Point broadcasting eduroam, configured to connect to their rogue RADIUS server), eduroam user devices will typically automatically associate with the rogue AP, and an authentication transaction will commence. If the user’s eduroam configuration disables home RADIUS server authentication, or if the user continues the transaction (e.g. accepts the rogue RADIUS server certificate), if the inner-authentication PAP, the user’s credentials will be delivered to the rogue RADIUS server. Even if using MSCHAPv2 (encryption used for user credentials) for innerauthentication, the user may also be exposed to a man-in-the-middle attack exploiting a known MSCHAPv2 vulnerability.