Homework lecture 8
Mobile telephony security

Harald Vranken
harald.vranken@ou.nl
April 15, 2019

Question 1
When roaming (i.e., using your mobile phone in a foreign country, or using it within your country but with a different provider's network), which provider is in charge of authentication?

Answer
Your phone communicates with a cell tower in reach, which is operated by some provider A that operates the local *access network*. Your phone provides your (actually, the SIM's) IMSI (International Mobile Subscriber Identity), which identifies your *home network* (operated by your provider B). Provider A will contact provider B, and provider B will do the authentication. (See figure 2.1 and corresponding text on page 16-17 of Fabian's PhD thesis.)

Question 2
3GPP networks provide both authentication and encryption. Is authentication or encryption more important for providers? And for users?

Answer
For providers, authentication is more important, since their billing process depends on authentication. Encryption is of no direct importance for providers.
For users, authentication and encryption are both important. As a user, you only want to pay for your own phone usage and not for someone else's, and also you want to be sure that you cannot be spoofed. You also want to be sure that your messages cannot be eavesdropped or modified.

Question 3
In 4G the signalling connection is secured between the phone and the signalling gateway, while the user data connection is secured between the phone and the cell tower. What is the reason for this difference?

Answer
This setup was chosen to allow cheaper handovers between connected cell towers, as the encryption and integrity key for the user data connection can be forwarded between directly connected cell towers. (See page 19 of Fabian's PhD thesis.)

Question 4
Consider the man-in-the-middle attack (see slide 28). Why/how is the man-in-the-middle able to decrypt and encrypt the traffic?

Answer

The weakness exploited is in fact that the session key used in A5/2 is the same as in A5/1 and A5/3.
The network first sends an authentication request and a challenge (RAND) to the MITM, which the MITM forwards to the victim. The victim computes the response, and returns it to the MITM. Next, the MITM asks the victim to encrypt with A5/2, which the victim considers to be a legitimate request. The MITM now employs cryptanalysis of A5/2 to retrieve the session key used by the victim. Finally, the MITM sends the authentication information to the network.
Since the session key only depends on RAND, the key recovered through the A5/2 cryptanalysis is the same key to be used when A5/1 or A5/3 is used. The MITM therefore can encrypt/decrypt with A5/1 or A5/3 using this key. Note that this attack can go unnoticed, since the GSM standard allows 12 seconds for the phone to complete the authentication calculations and to return an answer, while the delay incurred by this attack is less than a second. (See page 34-35 of Fabian's PhD thesis.)