IT Security 2024/2025
Exercise Sheet 3
Security of Distributed and Resource Limited Systems

Dr. Thorsten Aurisch

Publication: 24.10.2024
Deadline: 30.10.2024 10:00

Lightning Survey ⚡

Submit your solutions as `answers.pdf` to the repository.

Exercise 1 (Explain in your own words, 1+1+1 points)**.**

a) Write down the Needham-Schroeder protocol and explain the weakness of the protocol in case of a stolen session key and a man-in-the-middle attack.

b) Explain the two different types of secret sharing from the lecture.

c) Explain the basic operation of a blockchain-based distributed ledger.

Exercise 2 (Distributed Group Key Management, 2+1+2 points)**.**

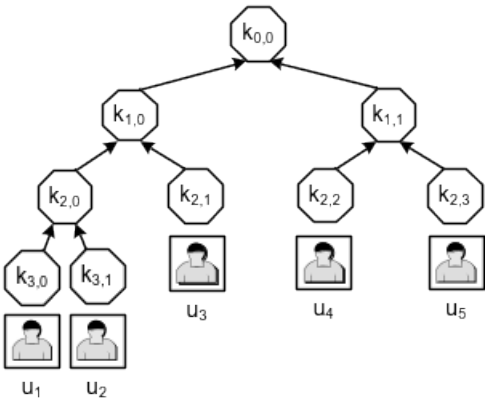

Figure 1: Key tree of the TGDH protocol

Given is the group $\mathbb{Z}_{37}^*$ with generator $g = 2$. The users u_1, u_2, u_3, u_4, and u_5 use the Tree-based Group Diffie-Hellman (TGDH) protocol with the key tree shown in Figure 1 for the group key establishement. Assuming that the following keys are stored in the leaves: $k_{3,0} = 9$, $k_{3,1} = 5$, $k_{2,1} = 8$, $k_{2,2} = 17$, $k_{2,3} = 27$.

a) The user u_6 with the key $k = 19$ joins the group. Draw the modified tree.

b) Write down the messages of the sponsor.

c) Now the user u_5 leaves the group. Hence, the user u_4 alters his private key to 10. Calculate the new group key.

Exercise 3 (Secret Sharing, 1+1 points)**.**

a) A one-time pad is the simplest 2-out-of-2 secret-sharing algorithm. Only the authorized set of users u_1 and u_2 can reconstruct the secret. Specify the algorithm and reconstruct the message from the shares $s_1 := 0110000011$ and $s_2 := 1011010111$.

b) Assuming five users $u_i,\ i = 1, 2, 3, 4, 5$ and a (3,5)-threshold sharing algorithm with the polynomial $f(x) = 15x^2 + 14x + 6 \mod 17$. Calculate a share for each user. Show that the secret can be restored by using the key shares of users u_1, u_2, u_3. (useful calculation rules: $(-a) \mod b = (kb - a) \mod b$, `https://de.planetcalc.com/8329/`).