TECHNISCHE UNIVERSITÄT WIEN
Vienna University of Technology

institute of telecommunications

Exercise 4: Encrypted Covert Data

Network Security - Advanced Topics (VU 389.160), Winter Semester 2018/2019

Communication Networks Group at the Institute of Telecommunications

Your suspicions about the usage of covert channels within the minister's office network to clandestinely convey information proved to be true after all. Your findings indicate that another covert communication is likely taking place right now and, according to the previously discovered message, it might even be encrypted this time. Quickly, you ask the network operators for the newest traffic captures of the minister's office network.

While gathering your team, a member of the ministry's security staff approaches. He informs you that another suspect was taken into custody and hands you a note (Figure 1) that was found in the suspect's pocket. Clearly, the security staff does not have the slightest clue about the meaning of the note. You, on the other hand, immediately recognize its value – this note might actually facilitate decrypting the covert message! The suspect furthermore carried a USB flash drive containing only one directory named "test", which might be helpful.

Finally, everybody in your team starts checking the most recent traffic files. All information you can disclose about the intruders and the transferred data are of utmost importance!

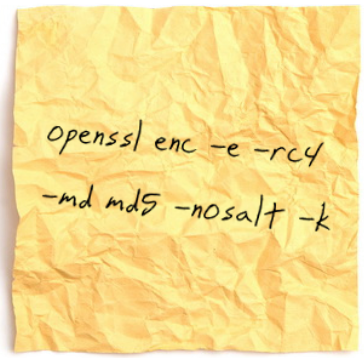

Figure 1. Note from the second suspect.

You can find the captured traffic as a pcap file to analyze in your `workfiles` folder (`/home/team??/workfiles/team??_ex4.pcap`). Also you'll find the test files for decryption there.

Rep:4.a – Encryption/Decryption

What does the note reveal about the encryption used? How can you use that information the decrypt the message? Is the employed encryption scheme secure? Is the security of the encryption scheme important (in this specific case)? Explain your answers!

Rep:4.b – Steps

Find, decode, and decrypt the covert channel. In the report, depict briefly every step so that your exploration can be understood and reproduced. For every step, provide sound arguments and reasoning that support your decisions. In addition, specify the information that characterizes the covert channel.

Note: Also, briefly comment on wrong attempts or approaches that did not lead to any improvement but allowed you to progress in your reasoning. Be short, accurate, and organized.

Rep:4.c – Message

Write in the report the message contained in the discovered covert channel.