Alon Towers 1, 36th floor
94 Yigal Alon st.
Tel Aviv, Israel 6789155
+972-77-899-5100
contact@argus-sec.com
www.argus-sec.com

ARGUS
CYBER SECURITY

Argus Network Research Challenge

The objective of this exercise is developing methods to characterize CAN BUS traffic, used for inter-vehicle communication, and then apply those methods to identify cyber attacks.

- Download exercise materials from here, zip password is **Z9j9H2UxlyR6**
- As an introduction, read pages 6-11 and 84-85 in the *car_hacking.pdf* document.
- We provide 4 recordings of vehicle network traffic, each is text file with the following format:
  Timestamp (msec) | msg ID | data length | data | source port #t
- The first two recordings contain 7 different message IDs, while the second pair contains only one message ID. A real vehicle contains a few hundreds of different message IDs, but we filtered most of them out to reduce file size, parsing time, and making the files easier to deal with.

Exercise 1

- Start with *reference_recording_01.txt*, this file includes only legitimate traffic. Try to characterize the behavior of each message id, write code (preferably python) to assist in your analysis.
- The file *attacked_recording_01.txt* is a recording of the same vehicle and message IDs, but it also includes injected messages. The attacker chose some of the IDs in the recording and injected his own messages with malicious data.
- Try to answer to following questions:
  - Which message ids were injected?
  - At what time each attack began and ended? Try to identify the injected packets

Exercise 2

- The *reference_recording_02.txt* recording contains only one ID - 0x20C. This message behaves differently than the IDs in the previous part, timing wise.
- Identifying the injected messages in *attacked_recording_02.txt* will be more difficult, so start with finding a pattern in the data (or part of it), and see if it helps.

Additional notes:

- Sample timestamps are sometimes inconsistent - the timestamp might reset or drop during the same file. Also, a message can disappear for long period of time and then show up again. For the sake of this exercise, it's recommended to treat any such inconsistency as a beginning of a new sample file.

Alon Towers 1, 36th floor
94 Yigal Alon st.
Tel Aviv, Israel 6789155
+972-77-899-5100
contact@argus-sec.com
www.argus-sec.com

ARGUS
CYBER SECURITY

- As mentioned in the article, the timing of messages is an important feature to work with.
- Document your thought process and your findings and send it to us together with any code you wrote.

Please let us know if anything isn't clear or if you have additional questions.
Good Luck!