## Toyota Motor Corporation, Toyota Motor North America, Inc. and Toyota Tsusho Systems US, Inc. organized an event for students

Toyota Motor Corporation (Toyota), Toyota Motor North America, Inc. (TMNA), and Toyota Tsusho Systems US, Inc. (TTS-US) have jointly organized "Hack Festa", an event designed to educate and promote automotive cybersecurity, which has been held annually since 2022. Hack Festa uses "PASTA for Education" and "RAMN", both developed by Toyota employees, as targets for participants to work on. In order to make it easier for participants to tackle the problems, we provide them in a "Capture The Flag" (CTF) format. This year, based on the experience of the past two years, we have added a European country to a participant and held the event in three countries at the same time.
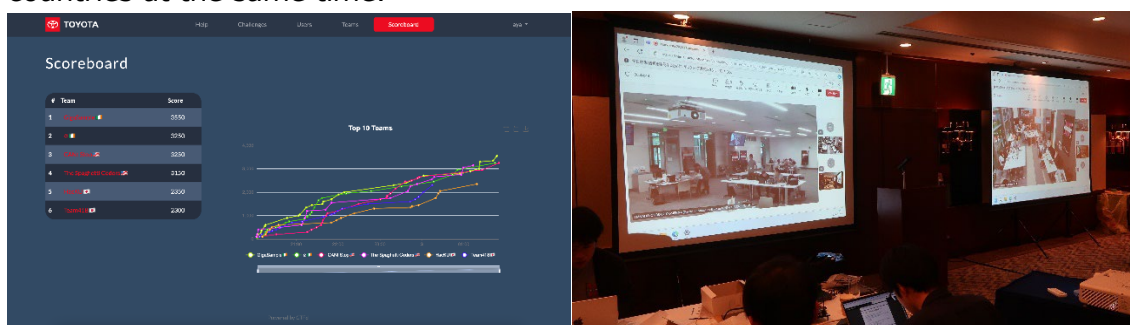

PASTA (Portable Automotive Security Testbed with Adaptability) 1.0[1][2] is a testbed for automotive cybersecurity research and development, and already available as open source. PASTA for Education follows the philosophy of PASTA 1.0 and it has advantage availability and portability rather than PASTA 1.0. As the same as PASTA 1.0, PASTA for Education also adopts general communication protocols for automotive. Therefore, the Toyota researchers expect to expand the usage of PASTA for Education, in particular education and CTF.

RAMN (Resistant Automotive Miniature Network)[3] is a PASTA-like testbed which is more conscious towards low-cost fabrication. Due to such excellent availability,

RAMN has been already adopted by overseas CTFs and automotive cybersecurity workshops[*4]. Also, hardware and software specification of RAMN has been already published as "Open Source Software" (OSS)[*5].
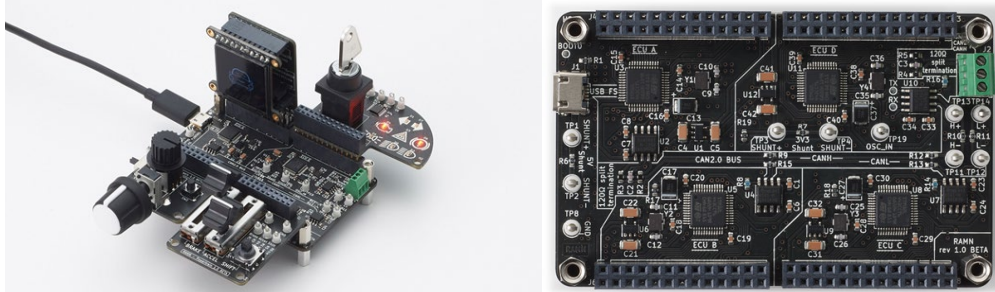
CTF is a kind of competition event in the information security field[*6*7]. Participants in a CTF take advantage of their expertise and skills to find hidden "Flags" (answers) in time and compete for the total number of points assigned for the flags which they have obtained. Also, the participants struggle with given "Challenges" (questions), which are sometimes solved in a quiz-like format and played as pseudo-offensive and defensive battles within a provided network at other times.

Nowadays, automotive industry must conform to United Nations Regulation No. 155 and ISO/SAE 21434 which is referenced from the regulation. They are sure that collaboration with hacking communities is a clue to solve such issues. Through operating of Hack Festa, Toyota, TMNA, and TTS-US aim to realize a framework for ethical hacking.

In contrast to the last two years, "Hack Festa 2024" has been revised with organizing qualifiers held in Japan, the United States, and Ireland, a new participant this year. The Irish qualifier was held on September 13 and 14, the Japanese qualifier on October 5 and 6, and the United States qualifier on October 18 and 19, respectively. Each qualifier was attended by five teams from one university in Ireland, nine teams from four universities in Japan, and eight teams from one university in the United States. Two representative teams from each country went to the championship. The championship was held on November 2, starting at 11:00AM Irish time, 8:00PM Japan time, and 6:00AM U.S. time, and ended successfully after six hours. During the competition, Ireland, Japan, and the United States were connected online to enable the events to be held simultaneously. Toyota and TMNA employees created challenges that were used in each country's qualifier and the championship, and assisted participants as local mentors.

Toyota, TMNA, and TTS-US will continue their activities relevant to cybersecurity for developing technologies which ensure the safety and security of all customers who use automobiles.

References

*1
GitHub – pasta-auto/PASTA1.0: PASTA: Portable Automotive Security Testbed with Adaptability
https://github.com/pasta-auto/PASTA1.0

*2

Portable Automotive Security Testbed with Adaptability PASTA

https://www.chip1stop.com/sp/products/toyota-pasta_en

*3

RAMN: Resistant Automotive Miniature Network

Hack In The Box Pte Ltd.

HITB+ CyberWeek 2020 Virtual Edition

Camille Gay, Tsuyoshi Toyama, and Hisashi Oguma

https://cyberweek.ae/2020/ramn-resistant-automotive-minimal-network/

*4

Car Hacking Workshop with RAMN Platform

https://infosecmap.com/listing/car-hacking-workshop-with-ramn-platform/

*5

GitHub – ToyotaInfoTech/RAMN: RAMN (Resistant Automotive Miniature Network),
a miniature CAN/CAN-FD testbed of 4 Electronic Control Units

https://github.com/ToyotaInfoTech/RAMN

*6

Automotive CTF 2024: Top Teams From Japan Advance to Global Finals in Detroit

https://vicone.com/blog/automotive-ctf-2024-top-teams-from-japan-advance-to-global-finals-in-detroit

*7

Crossing the Finish Line: Automotive CTF 2024 Champions Crowned in Detroit

https://vicone.com/blog/crossing-the-finish-line-automotive-ctf-2024-champions-crowned-in-detroit