CSC 497/583 Fall 2019 Reading Question 3

Dr. Si Chen

Kernel Exploit and the future of Software Security

First, if you are not familiar with Kernel Exploit, please check the following slides:

- ch23

- ch24

Please read the following article:

VER-THE-AIR: HOW WE REMOTELY COMPROMISED THE GATEWAY, BCM, AND AUTOPILOT ECUS OF TESLA CARS

Answer the following questions: in this attack, the authors claim that they find/use a 0-day kernel vulnerability to gain control the system.

Q1). Please explain why a linux kernel bug can be utilized to attack autonomous driving cars?

Q2). In this paper, the authors states "... the new 0-day vulnerability only exists in Tegra nvmap kernel module..." What's a kernel module? Why kernel module is the most common place to find vulnerabilities?

Submission

- Please upload your response **in PDF format** to D2L Assignmentbefore deadline. Late submission will not be accepted;

- The assignment should be submitted to D2L directly.