Automating Reverse Engineering of Automotive Networks

Charles Barron Kirby

University of North Georgia

Abstract

The purpose of this research is to automate the reverse engineering of an automobile's CAN bus. This will allow a better understanding of the communications that exist within modern car systems. Cars are becoming more and more reliant on computers to operate. However, these systems are not secure against hacking. As such, understanding the CAN Bus can provide a better understanding of an automobile's vulnerabilities. Reverse engineering a CAN Bus requires us to capture the CAN packets and send replay attacks to understand what the packet can affect, and on which component of the car. These replay attacks are done by capturing network communications and resending them to duplicate an action. This can be used on a CAN Bus to find the effects of resending selected packets. To automate this process, a Python script will take a packet capture file of CAN Bus packets sent inside the car. The script will then parse the packets to resend back to the car in a segmented fashion. The user can then identify what the packets are doing inside the car to reverse engineer the automobile's control systems.

Keywords: CAN (Controller Area Network), Vulnerability, Replay Attack, Networks, Kali Linux, Python, Reverse Engineering, Cyber Security, Automotive, Networks, Computers