Oct 20th, 10:55 AM - 11:20 AM

Car Hacking: CAN it be that simple?

Bryson Payne
University of North Georgia, bryson.payne@ung.edu

Follow this and additional works at: https://digitalcommons.kennesaw.edu/ccerp

Part of the Information Security Commons, Management Information Systems Commons, and the Technology and Innovation Commons

Abstract
The Internet of Things (IoT) has expanded the reach of technology at work, at home, and even on the road. As Internet-connected and self-driving cars become more commonplace on our highways, the cybersecurity of these "data centers on wheels" is of greater concern than ever. Highly publicized hacks against production cars, and a relatively small number of crashes involving autonomous vehicles, have brought the issue of securing smart cars to the forefront as a matter of public and individual safety. This article describes the integration of a module on car hacking into a semester-long ethical hacking cybersecurity course, including full installation and setup of all the open-source tools necessary to implement the hands-on labs in similar courses. The author demonstrates how to test an automobile for vulnerabilities involving replay attacks using a combination of open-source tools and a $20 commodity CAN-to-USB cable. Also provided are an introduction to the CAN (controller area network) bus in modern automobiles and a brief history of car hacking.

Location
KC 462

Disciplines
Information Security | Management Information Systems | Technology and Innovation

EXTENDED ABSTRACT

The Internet of Things (IoT) has expanded the reach of technology at work, at home, and even on the road. As Internet-connected and self-driving cars become more commonplace on our highways, the cybersecurity of these "data centers on wheels" is of greater concern than ever. Highly publicized hacks against production cars, and a relatively small number of crashes involving autonomous vehicles, have brought the issue of securing smart cars to the forefront as a matter of public and individual safety.

However, there has previously been a rather steep learning curve involved in applying cybersecurity research and teaching to car hacking. The purpose of this paper is to present a clear, step-by-step process for creating a car-hacking research workstation, whether on a laptop, in a virtual machine, or even on a Raspberry Pi. This article describes the integration of a module on car hacking into a semester-long ethical hacking cybersecurity course, including full installation and setup of all the open-source tools necessary to implement the hands-on labs in similar courses.

The OpenGarages.org ICSim, or Instrument Cluster Simulator, is a free, open-source package for car hacking and automotive security testing. The package relies the free Linux CAN Utilities *can-utils*, which are easily available using APT, rpm or other package management systems. After installing a few dependencies and the *can-utils* Linux CAN drivers, users can use git to download the ICSim tools and begin using a simulated car dashboard and CAN network. Viewing CAN packets can be achieved using any network sniffing tool, including Wireshark or the Linux CAN utility *cansniffer*.

Students and security researchers alike can experiment with a replay attack, a common vulnerability testing approach, by capturing packets in Wireshark or *candump*, using the ICSim controller to simulate commands going across the CAN network, and then replaying or re-injecting those packets across the CAN network. Many IoT devices have demonstrated replay attack vulnerabilities, and many automotive systems are similarly vulnerable once you have access to the CAN network in the automobile.

Finally, researchers and advanced students can connect their Linux car hacking workstation to any 1996 or newer automobile using a low-cost OBD-II (on-board diagnostic port version 2) to USB cable, like the $20-$30 OBDLink SX cable from ScanTool, available from Amazon, Walmart, and other retailers. The free ScanTool Linux drivers include the software needed to connect to automobiles from dozens of manufacturers worldwide. Wireless (Wi-Fi and Bluetooth) OBD-II port devices can be purchased for as little as $20-$50USD, and advanced penetration testers can attempt the same attacks via 4G LTE, Wi-Fi and Bluetooth connections without a direct OBD-II connection to the vehicle.

In short, the tools and techniques necessary for car hacking and automotive security testing are readily available, and the threat of attacks on automotive systems has been demonstrated to be real and ongoing. The goal of this paper is to give faculty, students, and researchers the ability to implement car hacking and automotive security testing in their own courses and lab environments.