reCAN: An Extensible CAN bus hacking methodology and software package

Christopher Hoder, Grayson Zulauf, Theodore Sumers, Sergey Bratus, Daniel Bilar, Travis Goodspeed, Andrew Righter

Why It's Cool:

Over the past decade, automobile electrical systems have evolved into complex networks of sensors and microprocessors, generally referred to as Electronic Control Units (ECUs). A typical, modern car contains between 50 and 70 ECUs, which are responsible for virtually every aspect of normal operation, from anti-lock braking to engine timing. These ECUs communicate with each other over the car's Controller Area Network (CAN) bus using the mandated CAN protocol standard.

This presents a vulnerability that can be exploited across all new automobiles, with the network accessed via a number of attack surfaces, from the OBD-II port to BlueTooth connections. With nearly every American driving daily, successful exploitation and control of the CAN bus presents a serious security issue, with potential threats to safety, security, and intellectual property.

Our project has developed a basic generalizable methodology and software package, allowing us to demonstrate the existence of serious flaws in the security of automobiles' CAN busses. With these initial capabilities, future users could easily begin reverse-engineering their own cars, as well as develop more elaborate hacks with more modern (and thus more connected) vehicles, fully exposing the vulnerabilities present.

While other groups have published more in-depth results, they have refused to release their codebase and methodologies for fear of malicious use. Further, these groups have relied on deconstruction of the individual ECUs in a lab setting, rendering their methodologies less applicable to a time-sensitive hack on a car.

Description of Presentation:

Using Travis Goodspeed's GoodThopter10 board to interface with the vehicles OBD-II port, the team developed a reverse-engineering methodology and a software package with which to implement this methodology. This generalizable methodology outlines a series of experiments to map out a given vehicle's CAN bus and to begin decoding the messages on it, ultimately concluding with an impactful hack on the vehicle.

Currently, the baseline software package provides a user interface to view, store, and analyze raw CAN data. Additional functionality includes integration with a SQL database, experimental documentation, basic fuzzing and other general experiments, and writing to .pcap format for eventual analysis in Wireshark. This interface also provides the user the ability to attach experimental modules for customized capabilities.

A proof-of-concept hack was carried out on a 2004 Ford Taurus, where the

team successfully reverse-engineered the manufacturer-specific CAN protocols and demonstrated repeatable hacks, including a complete denial-of-view attack in which we systematically manipulated every component on the dashboard.

Currently, the software is fully functional and provides a user interface to carry out these capabilities. In the next few weeks, we will rewrite our packet manipulation, using the Scapy package in Python, to mirror current standards used in Ethernet packet construction.

We plan to present our methodology and a brief introduction to how to use and build upon the existing open-source software package, as well as the exciting results achieved.

Supporting Materials:

Current codebase is included in the goodfet code package at goodfet.sourceforget.net. Our work specifically is contained within the goodfet/contrib/hoder and the goodfet/trunk/client directories.

PowerPoint presented to Thayer School review board attached to the email.

Software demonstration at:
http://www.youtube.com/watch?v=hpwBmTw7Gm0&feature=youtu.be
Capability demonstration at:
http://www.youtube.com/watch?v=p3-fjJZhACg

Experimental setup shown below, in Figure 1.

Figure 1: Experimental setup in a 2004 Ford Taurus, from the OBD-II port to the Goodthopter10 board to the laptop running our software package.

Presenter Contact Information and Biographies:

Christopher Hoder is a software engineer, graduating from Dartmouth College this year.
Cell: 617-823-0952
Email: chrishoder@gmail.com
Theodore Sumers is an embedded systems engineer who recently received his undergraduate degree from Dartmouth College.
Cell: 551-427-5793
Email: ted.sumers@gmail.com
Grayson Zulauf is an electrical and computer engineering major who will be graduating from Dartmouth College this June.
Cell: 970-708-9385
Email: grayson.d.zulauf@gmail.com
Sergey Bratus is a research assistant professor in the Computer Science Department at Dartmouth College, specializing in UNIX security.
Cell: _____
Email: sergey.bratus@dartmouth.edu
Daniel Bilar _____
Cell:
Email: daniel.bilar@siegetechnologies.com

VISA Considerations:

None required.

Travel Expenses:

No assistance required.