Penetration Test for Block Harbor

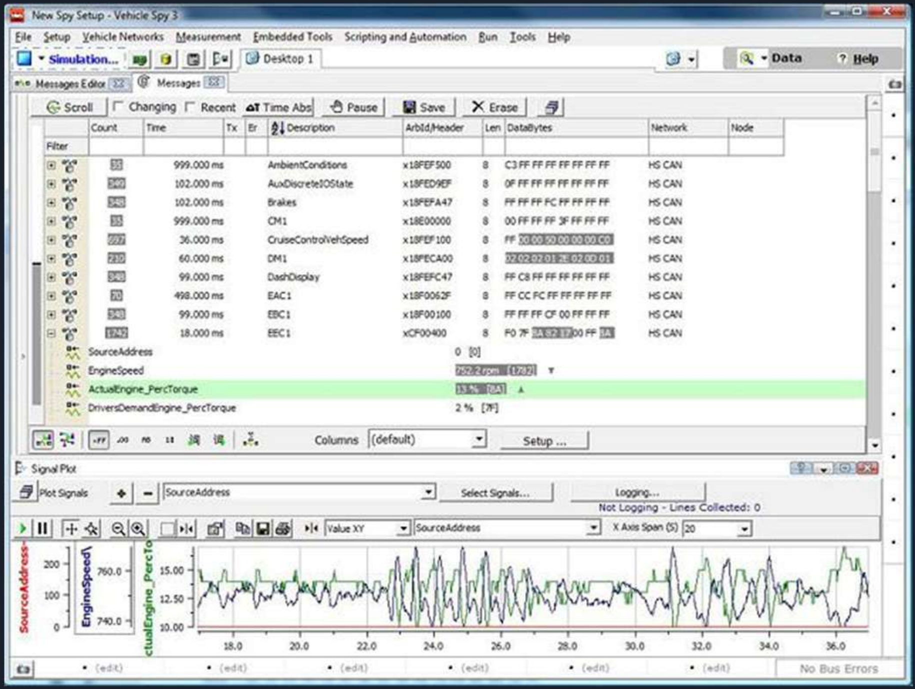
Jesse Russell, Yahia Khalaf, Hannah Hatala, and Cameron Keesee

Introduction/Executive Summary

Our team was tasked by Bryan Blancke at Block Harbor Cybersecurity to conduct a penetration test on a 2016 Jeep Cherokee. When this project began, our team had little knowledge on the topic of automotive security, but through a large volume of research and some testing, we were able to learn quite a bit about the functions of ECUs that reside in all modern vehicles. We learned how CAN functions, how it communicates over the vehicle’s network, CAN fuzzing (spoofing), and explored multiple tools to analyze the CAN traffic

Tools

1. Software
    a. Vehicle Spy
    b. Kayak
    c. CaringCaribou
    d. CAN-Utils/SocketCAN
    e. Instrument Cluster Simulator (ICS)
    a. Kali Linux
    b. WiTech Web Interface
    c. TeamViewer

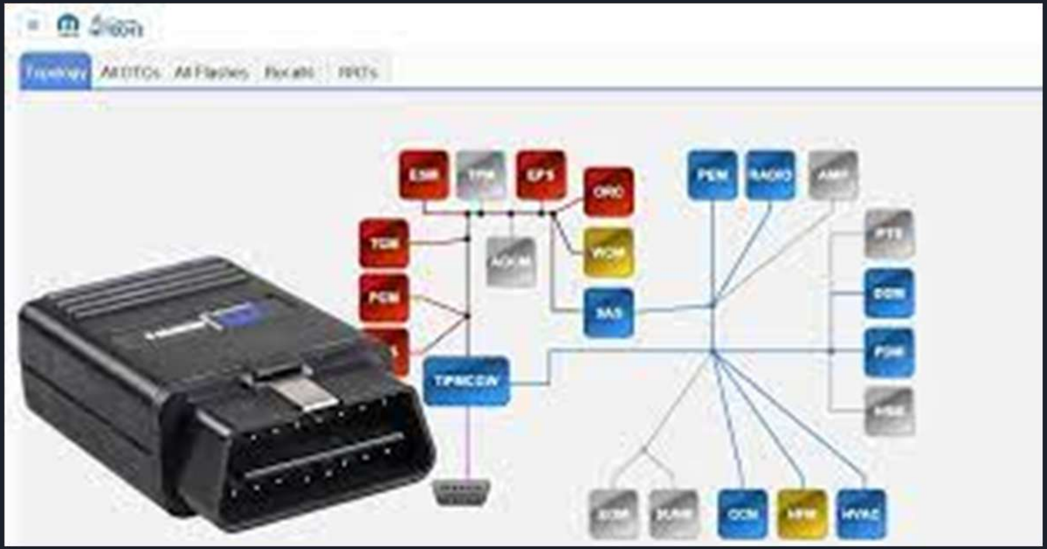


	Count	Time	Tx	Er	Description	ArbId/Header	Len	DataBytes	Network	Node
Filter										
	35	999.000 ms			AmbientConditions	x18FEF500	8	C3 FF FF FF FF FF FF FF	HS CAN	
	349	102.000 ms			AuxDiscreteIOState	x18FED9EF	8	0F FF FF FF FF FF FF FF	HS CAN	
	348	102.000 ms			Brakes	x18FEFA47	8	FF FF FF FC FF FF FF FF	HS CAN	
	35	999.000 ms			CM1	x18E00000	8	00 FF FF FF 3F FF FF FF	HS CAN	
	697	36.000 ms			CruiseControlVehSpeed	x18FEF100	8	FF 00 00 50 00 00 00 C0	HS CAN	
	210	60.000 ms			DM1	x18FECA00	8	02 02 02 01 2E 02 00 01	HS CAN	
	348	99.000 ms			DashDisplay	x18FEFC47	8	FF C8 FF FF FF FF FF FF	HS CAN	
	70	498.000 ms			EAC1	x18F0062F	8	FF CC FC FF FF FF FF FF	HS CAN	
	349	99.000 ms			EBC1	x18F00100	8	FF FF FF CF 00 FF FF FF	HS CAN	
	1742	18.000 ms			EEC1	xCF00400	8	F0 7F 8A 82 17 00 FF 8A	HS CAN	
SourceAddress							0 [0]			
EngineSpeed							752.2 rpm [1782]			
ActualEngine_PercTorque							13 % [8A]			
DriversDemandEngine_PercTorque							2 % [7F]			

Not Logging - Lines Collected: 0

Tools

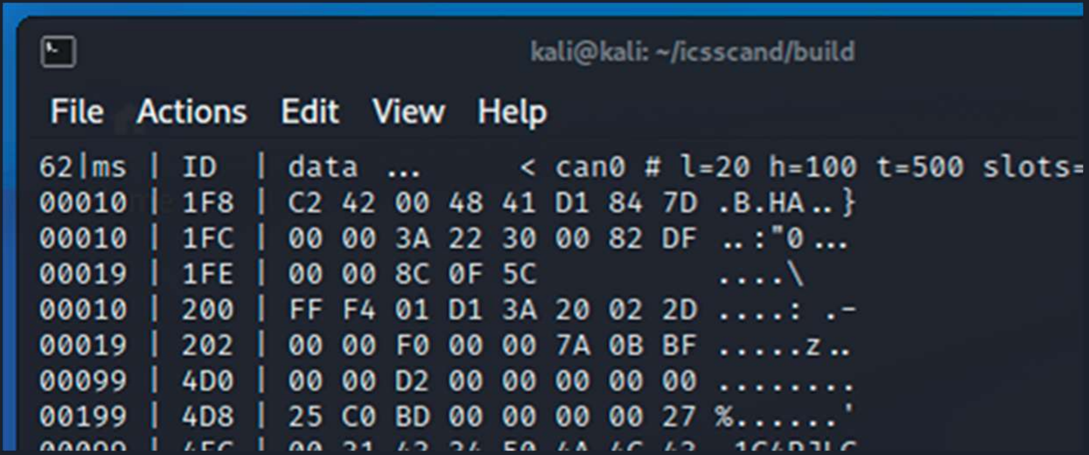
1. Hardware
   a. WiTech 2.0
   b. ValueCan
   c. Simulated Vehicle Module



Tools - CAN-UTILS

a. **CAN-Utils/SocketCAN-** A suite of tools that provide a basic framework for looking at the CAN traffic. Often, other CAN analyzers will require this to be installed as a prerequisite.

a. The CAN-Utils program was used in order to capture raw CAN traffic from the vehicle, as seen in the screenshot below. Depicted is the output of the CANSNIFFER command offered Within the CAN-UTILS suite.

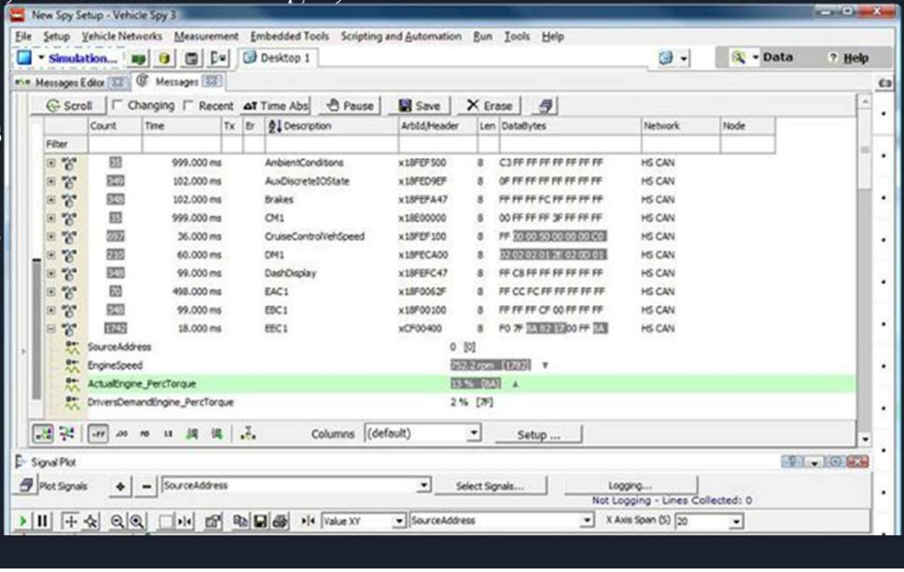


```
62|ms | ID  | data ...      < can0 # l=20 h=100 t=500 slots=
00010 | 1F8 | C2 42 00 48 41 D1 84 7D .B.HA..}
00010 | 1FC | 00 00 3A 22 30 00 82 DF ..:"0...
00019 | 1FE | 00 00 8C 0F 5C             ....\
00010 | 200 | FF F4 01 D1 3A 20 02 2D ....: .-
00019 | 202 | 00 00 F0 00 00 7A 0B BF .....z..
00099 | 4D0 | 00 00 D2 00 00 00 00 00 ........
00199 | 4D8 | 25 C0 BD 00 00 00 00 27 %......'
```

Tools - Vehicle Spy 3

a. Vehicle Spy 3- An enterprise Windows application used to intercept and analyze CAN traffic in a neat and presentable GUI, typically used with a device such as ValueCAN.

Vehicle Spy has the ability to graph data, send/receive messages, decode arbitration IDs with DBC files, etc. The following screenshot displays The user interface of Vehicle Spy in this Instance outputting the various signals Discovered over the module such as the, Cruise control, brakes, and dash display.



Filter	Count	Time	Tx	Er	Description	ArbId/Header	Len	DataBytes	Network	Node
	35	999.000 ms			AmbientConditions	x18FEF500	8	C3 FF FF FF FF FF FF FF	HS CAN	
	349	102.000 ms			AuxDiscreteIOState	x18FED9EF	8	0F FF FF FF FF FF FF FF	HS CAN	
	348	102.000 ms			Brakes	x18FEFA47	8	FF FF FF FC FF FF FF FF	HS CAN	
	35	999.000 ms			CM1	x18E00000	8	00 FF FF FF 3F FF FF FF	HS CAN	
	997	36.000 ms			CruiseControlVehSpeed	x18FEF100	8	FF 20 00 50 00 00 00 C0	HS CAN	
	210	60.000 ms			DM1	x18FECA00	8	02 02 02 01 2E 02 00 01	HS CAN	
	348	99.000 ms			DashDisplay	x18FEFC47	8	FF C8 FF FF FF FF FF FF	HS CAN	
	70	498.000 ms			EAC1	x18F0062F	8	FF CC FC FF FF FF FF FF	HS CAN	
	348	99.000 ms			EBC1	x18F00100	8	FF FF FF CF 00 FF FF FF	HS CAN	
	1742	18.000 ms			EEC1	xCF00400	8	F0 7F 8A 82 17 00 FF 8A	HS CAN	
	SourceAddress						0 [0]			
	EngineSpeed						752.2 rpm [1782] ▼			
	ActualEngine_PercTorque						13 % [8A] ▲			
	DriversDemandEngine_PercTorque						2 % [7F]			

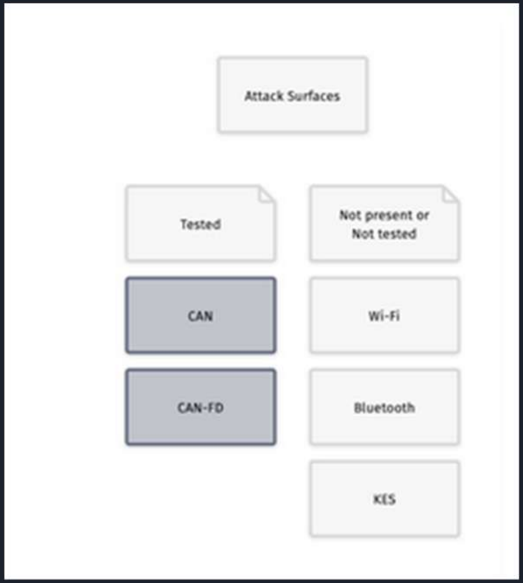
Plot Signals: SourceAddress

Not Logging - Lines Collected: 0

Value XY | SourceAddress | X Axis Span (S) 20

Methodology

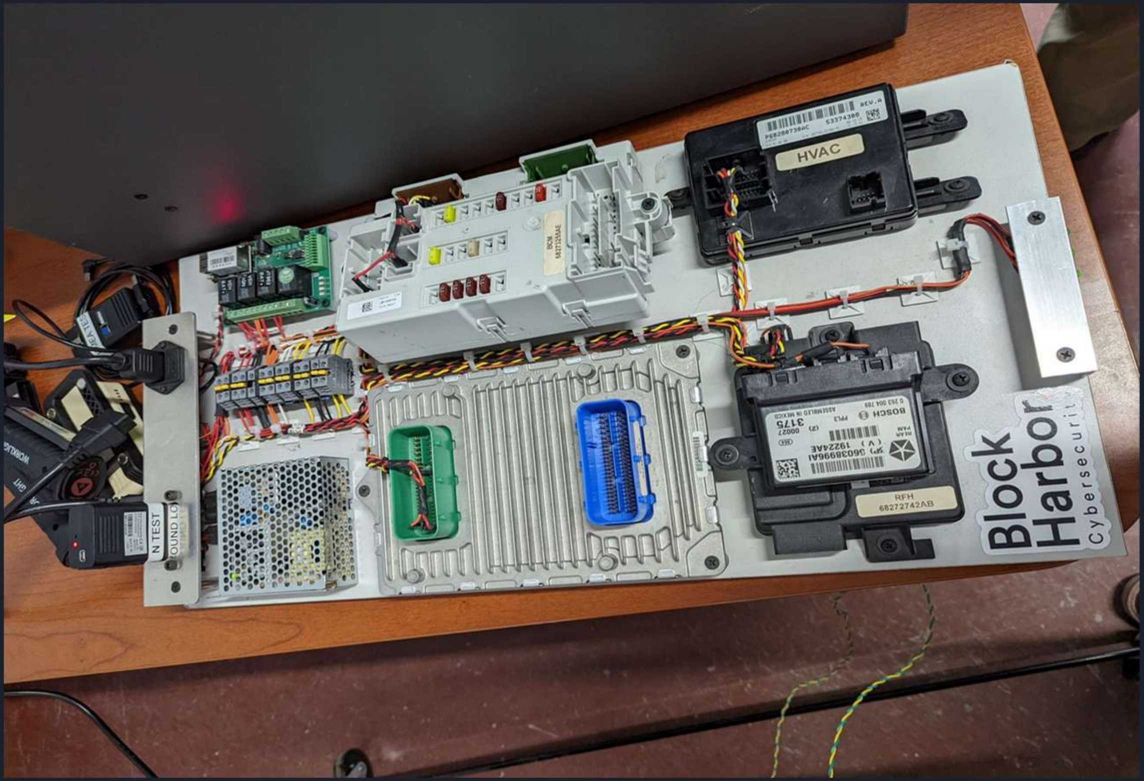
1. Threat Modeling
2. Passive Reconnaissance
3. Security Defense Checking
4. Active Exploitation
5. Deep Exploitation
6. Report Writing



Attack Surfaces

Tested	Not present or Not tested
CAN	Wi-Fi
CAN-FD	Bluetooth
	KES

Vehicle Module



Modules/ECUs

PAM (Parking Assist Module)

The Parking Assist Module (PAM) is used by the vehicle to facilitate features such as lane detection, automatic parking, brake warning/auto brake, and steering.

Possible Exploits:

- Once an attacker has access to the PAM inside a vehicle, they could then be able to control the entire vehicle and cause it to drive without any user interaction required. This presents an obvious safety hazard, as vehicles can be dangerous without complete control by the driver. If a customer were to be attacked in this way, they may be more likely to be in an accident causing injury or death.

PCM (Powertrain Control Module)

The Powertrain Control Module (PCM) is the ECU responsible for ensuring the engine runs smoothly, managing aspects such as gear control, speed control, fuel injection sensors, O2 sensors, etc. It has over 100 functions of control for the vehicle, and if any of those fail, the PCM will send a check engine light to the dashboard.

- **Possible Exploits:**
  - If the PCM is accessed, attackers may be able to control various functions of the vehicle's engine mechanisms such as shifting and fuel consumption. It may be possible to block the car from shifting or trick the vehicle into thinking it's in an entirely different gear altogether.
  - An attacker may be able to reduce fuel mileage, or even cause a fire, by injecting too much fuel into the cylinders, causing the engine to work harder than it needs to.
  - The engine's power may also be vulnerable to attackers through the PCM, causing the vehicle to slow down or speed up depending on the attacker's goal.

Modules/ECUs

BCM (Body Control Module)

The Body Control Module (BCM), in a basic sense, is the central computer in the vehicle that moderates communications between other ECUs in the system. For CAN messages, it works as a router to determine where to send packets on the network. Because the ECUs are intended for specific purposes, the BCM is a vital component that issues commands for the ECUs to execute. It also controls the physical power features in the vehicle, including power locks, power windows, windshield wipers, headlights, etc.

- **Possible Exploits:**
  - Access to the BCM could allow an attacker to try and distract the driver by causing malfunction in various powered devices in the vehicle. For example, if an attacker wanted to reduce the visibility of the road from the driver, they would only have to activate the windshield wiper fluid to render the windshield unusable.
  - An attacker may be able to remotely unlock the vehicle and allow a thief to enter.

Modules/ECUs

HVAC (Heating Ventilation and Air Conditioning)

The HVAC module is exactly what the name implies. It controls the interior air quality for driver/passenger comfort, including cabin temperature, fan speed, circulation, and defrost. Newer models of vehicles may feature heated/cooled seats, which would also be handled by the HVAC unit.

- **Possible Exploits:**
  - Once the HVAC module is accessed, an attacker may be able to disable certain functions of the vehicle’s climate system. For example, if that attacker wanted to raise the temperature inside to an unreasonably high amount, the passengers may be endangered and become severely dehydrated.
  - The attacker may also control aspects of the vehicle such as window defrost, which may cause the driver to lose visibility during a cold and rainy day.
  - If the heated seats are controlled remotely, an attacker may be able to burn the passengers by exploiting and modifying the heating element inside the seat.

Modules/ECUs

RFH (Radio Frequency Hub)

- ○ Throughout a vehicle’s network, certain radio frequencies must be generated for features to work properly. The Radio Frequency Hub (RFH) generates and receives these frequencies. For instance, on most vehicles built after 2013, keyless start is a standard feature that uses an NFC field to ensure a serialized chip is inside the vehicle. If this chip (located inside the key), is not present, the vehicle will not start.
- ○ **Possible Exploits:**
  - ■ Attackers may spoof the key’s NFC frequencies to trick the vehicle’s immobilizer into starting the vehicle without the proper serialized key present.
  - ■ Lane departure and lane assist systems use IR frequencies generated by the RFH. Attackers could diable these features to stop working entirely, or send a false flag to the system in order to cause the vehicle to stop prematurely.

Issues

- Time constraints
- Very little knowledge on pentesting
- Very little knowledge on Vehicle Analysis Tools
- Unsuccessful on finding DBC file
- Equipment mishaps

Feedback

- Better Beginning of semester briefing of project
- Communication with client right off the start in case of important questions that may arise during the first week of the project
- Important to remember that this is a learning process for the students and most of the time, they don’t have a clue of where to start or where to go
- Establishing clear guidance for the students

Conclusion

Our group's initial plan was to go through each phase of the penetration testing methodology provided by Block Harbor Cybersecurity, but we were unsuccessful in testing past the passive reconnaissance stage due to time limitations and the issues listed in the previous section. While the outcome did not reach our expectations, we were able to gain an understanding of the vehicle and learn more than we thought possible. Our project was inspired by the 2014 Jeep penetration test performed by Charlie Miller and Chris Valesek, in which they used the head unit to execute commands and exploit the vehicle. We all enjoyed learning about the penetration testing process and the mechanisms that allow modern vehicles to function. We were able to create a threat model through careful research, enumerate the attack surfaces, list all ECUs connected, learn how CAN works, and think like a professional penetration tester.