Car Hacking





About me

Daan Keuper

- Security researcher at Computest
- Followed the Kerckhoffs security master
- Currently working on car hacking
- Won Pwn2Own by hacking the iPhone
- Member of the Eindbazen CTF team





Security

OUR EXPERTISE



Performance



Functional Test automation







Chaos Lab a research lab where we conduct various research projects





Ansible

- Ansible is agent-less
- · Uses push instead of pull
- The controller uses SSH to control a node
- Just copies and runs series of Python scripts
- · Uses the Jinja2 template engine
- file: {{ ansible_distribution }}.conf
- + file: {{ lookup('pipe', 'uname -s') }}.conf















© 0.24.3 •• 83d51ae

0.24.3

dbarrosop released this on Jul 12 · 21 commits to develop since this release

This release fixes a minor issue where a network device with a compromised firmware could craft a string that would be evaluated as python code.

Downloads

Source code (zip)

Source code (tar.gz)





vagrant (vagrant)



I







Connected cars

- ~35% of all new cars were internet connected in 2015
- These cars will be on the road until ~2030!
- Experts estimate that in 2020 almost all new cars will come with internet connectivity

But, even without internet, your car is probably already a lot more connected than you might think



















CAN bus protocol

- There is no authentication, encryption etc
- Once you're on the bus, you can send/ impersonate whatever/whoever you want
- So, theoretically: if you are on the bus, you control the car

etc v vant



However...

- Difficult to know what controls what
- The original device will send contradicting messages
- Car's tend to choose for the safest option
- Some systems won't operate above a certain speed
- More importantly: most cars have • separated busses



















Collisions

- There is no clock signal, so high chance on collisions
- 0 is dominant (this is because lower ID's represent higher priority)
- Other device will pick up the transmission error and wait
 - 32 errors: passive state
 - 128 errors: go offline
- So an attacker can create an effective DoS





Preliminary conclusions

- In practise: if an attacker can send arbitrary CAN messages, he or she controls everything on that bus
- The gateway is software, which of course might contain vulnerabilities
- Conclusion: you don't want to give an attacker CAN bus access :)







Attack surface

- Key fob
- TPMS
- ODB-II (telematics)
- IVI system:
 - Cellular
 - Wi-Fi
 - Bluetooth
 - USB
- Vehicle-to-Vehicle (DSRC)



Key fob

- The new hotwiring
- Cryptographic attack:
 - e.g. Megamos Crypto key fobs: 2⁹⁶ reduced to 2⁵⁶ or even 2³⁷
- Physical attack to exposed CAN bus lines
- Relay against keyless entry/start
- Vulnerabilities could allow CAN bus access









TPMS

- Legally required on all cars
- Close range
- Radio signals, but Bluetooth is also used
- Broadcast every 60-90 seconds •
- Spoofed packages can shutdown the engine, or force it into "limp mode"
- Vulnerabilities could allow CAN bus access



ODB-II

- Legally required on all cars
- Used for diagnostic purposes
- Connected to the CAN bus
 - Direct access to all rings
- Growing market for telematics dongles (insurance companies, lease contractors etc)
- Typically have cellular connection



IVI system

- By far the largest attack surface:
 - Cellular
 - Wi-Fi
 - Bluetooth
 - Audio decoding
 - RDS/TMC etc
 - Browsers
 - etc...





Comprehensive Experimental Analyses of Automotive Attack Surfaces

Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, and Stefan Savage University of California, San Diego

Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno University of Washington

Abstract

This situation suggests a significant gap in knowledge, Modern automobiles are pervasively computerized, and and one with considerable practical import. To what exhence potentially vulnerable to attack. However, while tent are external attacks possible, to what extent are they previous research has shown that the *internal* networks practical, and what vectors represent the greatest risks? Is the etiology of such vulnerabilities the same as for within some modern cars are insecure, the associated threat model—requiring *prior physical access*—has desktop software and can we think of defense in the same manner? Our research seeks to fill this knowledge gap justifiably been viewed as unrealistic. Thus, it remains an open question if automobiles can also be susceptible to through a systematic and empirical analysis of the remote *remote* compromise. Our work seeks to put this question attack surface of late model mass-production sedan. We make four principal contributions: to rest by systematically analyzing the *external* attack surface of a modern automobile. We discover that remote **Threat model characterization.** We systematically exploitation is feasible via a broad range of attack vectors synthesize a set of *possible* external attack vectors as a function of the attacker's ability to deliver malicious (including mechanics tools, CD players, Bluetooth and cellular radio), and further, that wireless communications input via particular modalities: indirect physical access, channels allow long distance vehicle control, location short-range wireless access, and long-range wireless tracking, in-cabin audio exfiltration and theft. Finally, we access. Within each of these categories, we characterize discuss the structural characteristics of the automotive the attack surface exposed in current automobiles and their surprisingly large set of I/O channels. ecosystem that give rise to such problems and highlight

ANDY GREENBERG SECURITY 07.21.15 06:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT



I WAS DRIVING 70 mph on the edge of downtown St. Louis when the exploit began to take hold.

Though I hadn't touched the dashboard, the vents in the Jeep Cherokee started blasting cold air at the maximum setting, chilling the sweat on my back through the in-seat

Team of hackers take remote control of Tesla Model S from 12 miles away

Chinese researchers were able to interfere with the car's brakes, door locks and other electronic features, demonstrating an attack that could cause havoc



Now that cars such as Tesla's are increasingly high-tech and connected to the internet, cybersecurity has become as big an issue as traditional safety features. Photograph: Jim Dyson/Getty Images

Three months since the first fatal crash involving a Tesla driving in autopilot mode, hackers have taken remote control of a Tesla Model S from a distance of 12 miles, interfering with the car's brakes, door locks, dashboard computer screen and other electronically controlled features in the high-tech car.

A team of Chinese security researchers - Samuel LV, Sen Nie, Ling Liu and Wen Lu from Keen Security Lab - were able to <u>target the car wirelessly and remotely</u> in an attack that could cause havoc for any Tesla driver.

The hack targeted the car's controller area network, or Can bus, the collection of connected computers found inside every modern vehicle that control everything from its indicators to its brakes. In a video demonstrating the vulnerability, the hackers targeted both the <u>Tesla</u> Model S P85 and Model 75D, although they said it would work on other models too.

Research Goals

- A remote attack
- Requires no user interaction
- From here, work up our way to the highspeed CAN bus







1. ./exploit.py 89.200. (Python)



CPU A

ethernet















Impact

- Remote access to the IVI system
 - GPS location
 - Control speakers/screen
 - Activate microphone
- IVI system is shared between models
 - Remote works sometimes
 - USB always works



Conclusions

- Getting it right is hard
- There are benefits from having an (internet) connected car
- We don't want to/can stop this
- It is also logical that cars have an internal network, which include brakes, steering etc.



However

- It is all software; security vulnerabilities will always be a risk
- *Most* cars don't have an over-the-air update mechanism
- We can fix this for the car of tomorrow
- But what about all current cars on the road? They will still be here in 15 years



Thank you for listening

dkeuper@computest.nl

Game On Computest

