Lifting the Sheets on Automotive Embedded Control Systems

Tim Brom
Senior Security Researcher, GRIMM
Overview

- Todays cars are a moving network of computer systems
- Wide variety of technologies
- The technology is changing quickly
- Why do we care?
- How do we get started?
Wireless Attacks

- WiFi
- Bluetooth
- TPMS
- V2X
- RKE
- AM/FM Radio
Wired Attacks

- CAN
- CAN-FD
- LIN
- Automotive Ethernet
- Flex-Ray
- J1850, KWP (older)
How to Get Started

- To hack a car, you need a car
- Or something that is sufficiently like a car
Setting Up a Lab

- Creating a lab is a time-proven way to enhance skill and abilities
- Identify necessary components
- Get a wiring diagram and shop manual
- Wire it all together and get hacking
- Portability?
Getting Components

- Individual parts may not work together
- Parts from a junked car are already programmed to work together
Tools

- Macchina M2
- WiFi with Monitor Mode
- Bluetooth dongle/Ubertooth One
- SDR
- USB Serial Adaptor
- Bus Pirate/Shikra
- Logic Analyzer
- Oscilloscope
Software

- Manufacturer-provided diagnostics software (e.g., FMP)
- J2534 dongle (e.g., Drew Technologies Mongoose)
- Reverse-engineering tools (IDA, Binary Ninja, Radare2)
- CanCat
- Wireshark
Hacker’s Motivation

- Modern-day hackers are generally motivated by money
- Nation-states are motivated by national interest
- Doesn't mean we can ignore the "because I can" element
Financial Reasons to Hack

- Shorting OEM stock before a breach announcement
- Ransomware (you must pay 1 BTC to turn on your car)
Nation States

- Targeted Assassination
- Surveillance
- Tracking
A Little History

- First carputers
- Networking them
- Introduction of CAN bus
- Mandating OBD-II, CAN bus
- University of Washington car hacking research - ignored
- Chris and Charlie - not ignored
Automotive Security Challenges

- Basic security principles can be costly when you don’t have control over the system
- Patching, updating stability, regulatory concerns
- Applying patches to offline systems
- Validating updates
- Cost
Attacker Mindset

- How does an adversary think about attacking a car?
- They'll focus on something familiar
- What does a hacker see when they approach an IVI system?
What We Can Do

- Limit network accessibility
  - Having the IVI be the center of managing network connectivity makes limiting this connectivity harder
- Use strong passwords (or don't rely on passwords at all)
- Ensure services are running under accounts with limited permissions
What We Can Do

- Ensure debugging code and services are disabled in production
- Disable unused USB peripherals
  - Don't allow keyboards, ethernet cables to be plugged into the IVI
- Use encryption effectively
  - Understand encryptions strengths and weaknesses
- Segment networks
Thank You!
Questions?

Tim Brom
@b1tbane
Senior Security Researcher, GRIMM