CyberSecure Shop

An Initiative to educate automotive service providers to protect their business and customers from cyber attacks

Prepared by: Donny Seyfer AAM
10/30/2016
As more vehicles are built with direct or indirect connections to the Internet there is a growing need to consider the automotive repair shop as a possible attack vector and cyber security risk.

The Internet of Things
An Explosion of Connected Possibility

50 Billion by 2020
Avoid Becoming a Victim of Cyber Attacks by NOT Being an Easy Target
There is strong experiential evidence indicating that most repairers have not considered the possibility that their customer’s vehicles could be attacked in several possible ways during service in an auto repair or collision shop.
Many service repair shops provide their customers with wireless internet service while they are waiting for service.
Most of these networks do not employ the latest security measures and often provide easy access to the repair shop’s management system and internet connected scan tools resulting in potential PII and Vehicle network exposure.
During repair operations as simple as alignment or oil service, tools may be used to access the vehicle through the OBDII port.

This equipment is often internet connected either during the operation or during firmware updates.

When connected to a Controller Area Network equipped vehicle the potential exists for automotive targeted malware to be unknowingly planted on the vehicle network.
Let’s look at how a repair shop can unknowingly assist “bad guys”

To infect and potentially take control of vehicle network
Vehicles That Have Shown Susceptibility

- 2013-15 Jeep and Dodge Platform SUV/Charger
- 2014 Prius
- 2014 Escalade - On Star /Bluetooth
- 2014 Ford Fusion Sync
- Infiniti Center Stack resulting in Steering/Braking control

Systems accessed:
- Navigation
- Braking
- Steering
- Door Lock/Windows
- Remote access
Vehicles That Have Shown Susceptibility

Distances for Hacking Car Features

- Passive anti-theft system: 10 meters
- Bluetooth: 10 meters
- Radio data system: 100 meters
- Tire Pressure monitoring system: 1 meter
- Smart key: 5-20 meters
- In-car Wifi: Varies

ILLUSTRATION: CNNMONEY
One Example

2013-15 Jeep

- FCA issued a software update for U-Connect on 1.4 Million.
- Owners instructed to download and apply the security patch themselves.
- How many do you think were actually performed?
- All of this attention has made OE’s VERY cautious.
NHTSA encouraged the industry to create the Auto-ISAC and invite all stakeholders to participate.

Jan 2016 the Auto-ISAC began.

ISAC is an information sharing and analysis center initiative.

Much of it is anonymous to allow competitors to share problems they have discovered.
October 24, 2016
NHTSA on behalf of US-DOT published a best practices paper with recommendations for the auto industry

Among the recommendations were some general suggestions for auto service.
6.7 Fundamental Vehicle Cybersecurity Protections

The following recommendations are based on what NHTSA has learned through its internal applied research as well as from stakeholder experiences shared with NHTSA. These recommendations do not form an exhaustive list of actions necessary for securing automotive computing systems, and all items may not be applicable in each case. These protections serve as a small subset of potential actions which can move the motor vehicle industry towards a more cyber-aware posture.
6.7.11 Control Wireless Interfaces

In some situations, it may be necessary to exert fine-grained control over a vehicle’s connection to a cellular wireless network. Industry should plan for and design-in features that could allow for changes in network routing rules to be quickly propagated and applied to one, a subset, or all vehicles.

It is easy to see how this recommendation could apply to avoid exploitation of a vehicle during access to the vehicle or diagnostics or service.
8. Aftermarket Devices

The automotive industry should consider that consumers may bring aftermarket devices (e.g., insurance dongles) and personal equipment (e.g., cell phones) onto cars and connect them with vehicle systems through the interfaces that manufacturers provide (Bluetooth, USB, OBD-II port, etc.). The automotive industry should consider the incremental risks that could be presented by these devices and provide reasonable protections.

Aftermarket device manufacturers should consider that their devices are interfaced with cyber-physical systems and they could impact safety-of-life. Even though the primary purpose of the system may not be safety-related (e.g., telematics device collecting fleet operational data), if not properly protected, they could be used as proxy to influence the safety-critical system behavior on vehicles. Aftermarket devices could be also brought on to all ages and types of vehicles with varying levels of cybersecurity protections on the vehicle side of the interface. Therefore, these devices should include strong cybersecurity protections on the units since they could impact the safety of vehicles regardless of their intended primary function.
The CyberSecure Shop

In October 2015 the Automotive Service Association board of directors began building a plan and consensus to create a program to educate repairers.

To date the following groups have joined an industry wide coalition to contribute human and intellectual capital to the project.
Create a self-paced online learn and test program

The industry will create a learning environment that will also test in an “open book” format to ensure that the concepts are understood.

This program could also be delivered in a live instructor led version online or at industry events. As we know, people have different learning styles.

Additionally, to assist in demonstrating the Service Sectors commitment to the process, completed tests will be tracked and reported to government entities.
Network Changes in the Shop

• Separate business machines, Guest Access and Scan Tool/IOT tools into 3 networks.
• Technician cell phones and devices that leave the building stay on Guest
• Only business machines are on that network
• Scan tools that will connect to cars are isolated and unnecessary ports closed along with limiting access to websites.
• This change cost me $400 to reconfigure my Cisco Switch and Meraki including creating printing farm