INSIGHTS

Cyber made simple.

one brightly cyber

ELECTRIC VEHICLES AND CYBER VULNERABILITIES

BY JAY BORDEN

Two years ago, we wrote about the risks due to the increasing number of computers and computer controlled functions in vehicles. Examples are blind spot warnings, lane departure warnings, GPS, connections to mobile phones for calls and playing of music, etc. These all represent potential entry points for hackers.

Since then, electric vehicles have grown in popularity and sales. However, their increased reliance on computers and software makes them a bigger target for cyber attackers.

There is a cyber security event where cyber professionals attempt to find vulnerabilities and compromise systems with a goal of helping make them more cyber safe. Last year a Tesla 3 was compromised in under 2 minutes!

This year the attack targets expanded past the vehicles to include charging stations, home chargers, an operating system called Automotive Grade Linux, modems and infotainment systems in the vehicles.

Why were these included? Because they operate on WiFi, wireless, or Bluetooth adding to the attack surface and represent ways to reach the primary systems of the vehicles, the steering, braking, door locks, environmental controls, and more.

How successful were they in finding vulnerabilities this year? Very successful! In the three days of the event over 50 vulnerabilities were found!

Let's look at the potential entry points. Vehicles separate functions into two main systems. One being the infotainment system including radio, navigation, link to phones, external networks, etc. The other is the control functions, brakes, steering, headlights, and more. Of course, each aspect of a system needs to talk to other aspects of that system. This is done through a Controller Area Network or CAN.

onebrightlycyber.com
(888) 773-1920
A global leader in cyber service, technology, insurance and innovation.

INSIGHTS

Cyber made simple.

ELECTRIC VEHICLES AND CYBER VULNERABILITIES

Continued

It is basically the Internet of Things, IoT, for vehicles. However, the two systems, infotainment and controllers are not completely and totally separate from each other as they need to interact. This is where the attack surfaces multiply and increase the potential for interfering with the control systems.

Recognizing this, the industry is working to make the vehicles more cyber-safe. Two approaches are being explored for the infotainment systems as they are considered the easiest to attack due to the external network connections. The first is to use a mobile phone for the infotainment functions and only provide a large display in the vehicle.

The thinking here is that the phone manufacturers are experienced in keeping the devices cybersafe and have a mechanism in place to provide updates to the phones. Phones are also typically replaced more quickly than vehicles. By using the phone for those functions, it will be easier to keep it up to date and safer. From the car manufacturer's point of view, the phone belongs to the user, and it is their responsibility to keep it up to date.

The other approach is to get an operating system from one of the larger tech companies such as Google. These companies understand cybersecurity and understand how to keep systems up to date. Put that into the vehicle for the infotainment system and let the system provider keep it up to date.

The challenge we see with the second approach is most tech companies only offer support for 10 years. The life span of a vehicle is more than ten years although owners may change. When the car is sold or traded in, will there be any link to the user that needs to be deleted/changed? Who will update the systems beyond the ten year mark?

We have also seen tech companies discontinue products if they aren't selling well or no longer align with changes in technology or company direction. What happens to all the vehicles and people that rely on that system?

It should be clear by now that all vehicles have cyber security risks. Electric vehicles have additional risks due to the expanded reliance on software driven systems.

onebrightlycyber.com
(888) 773-1920
A global leader in cyber service, technology, insurance and innovation.

ELECTRIC VEHICLES AND CYBER VULNERABILITIES

Continued

We understand that there is nothing you can do to change this. Our goal is to make you aware of the risks and suggest you ensure patches and updates are installed as soon as possible whether they are user installed or have to be done by a dealer.

Don't forget to keep your phone up to date! It has the same network interfaces and connects to your vehicle.

Regardless of the system or technology chosen, you are the one who needs to see it is updated.

To learn all the ways we can help make your company safer, visit onebrightlycyber.com and contact onebrightlycyber at info@onebrightlycyber.com or call (888) 773-1920