Operating Systems
Spring Semester 2020

Greg Witt
greg.witt625@gmail.com

L-24

‘Plane Hacker’ Roberts: I put a network sniffer on my truck to see what it was sharing. Holy Crap!

Chris Roberts pleads for countries to rethink the security in their transportation sectors. As methods of transportation such as Cars and Planes have become more connected the necessity to protect the data and integrity of their systems shouldn’t become an afterthought. Cybersecurity for these devices in Israel are under threat constantly and the message of updating their systems for safety hasn’t gone unheard. This is particularly alarming as the Department of Homeland Security and NCCIS have put out warnings on air security and not much has been changed in the Air, Land or Sea industries. Robert’s has clearly mentioned the discussion of ECU reliability to the general public with OtA’s vulnerabilities. After putting a GPS data tracker on his device he uncovered that a lot of information was being shared without his knowledge. This opens the door to questions on ownership of this data as well. Does Ford, GM or Chrysler own it? Are they selling this information? Should you as a consumer be concerned with the data passing? Robert’s has gained the respect of the aviation industry through his alleged hacking of the United Airlines plane’s controls.

Toolset Enables Connected Vehicle Applications

A new toolset was enabled from Reneasas Electronics for applications developed on its R-Car SoC systems. These systems combine cloud-based data and vehicle data in order to offer driving prediction and assistance to drivers. These cloud connections are provided by

AWS and Greengrass . The applications have passed testing specifications from R-Cars for Automotive-Grade linux environments and meet W3C standards. All of these technologies are connected to an API that connects vehicle monitoring and various interfaces that send and receive information to and from the cloud. The interface allows for vehicle specific information such as surroundings, weather and road conditions. The Interface should work directly with open source languages such as Javascript and Python for additional development and deployment of additional services. All data elements such as conversations and driving habits can be recorded and tracked by AWS for continued support. There is even an emotional State Api that could sense the emotional stability of the driver in the car.

Why vehicle security may require a different approach

This article predicts that 152 Million vehicles will be connected to the internet by 2020. Hackers have a multitude of entry points, such as wifi, telematics and bluetooth. In 2018 Audi vehicles were hacked through wifi access. BWM was hacked through the same process in May of the same year, and even wiped the underlying OS of the IVN. This process was repeatedly noted in Tesla models as well. The attack is targeted at the ECU of these vehicles. Recommended methods manufacturers are taking include Not increasing boot time, securing low end devices, and expanding security to all elements of the devices controlled by the ECU. The main approach has been to utilize security features of OTA. This process would utilize cloud services but raises issues about RoT in the ECUs which require updating. Using only Secured ECUs would guarantee the safety of autonomous vehicles and prevent malicious attacks.

Executive Article Summaries

All of the Articles feature elements of transportation elements. The First article highlights the dangers and the vulnerable state of technology in all of the transportation sectors in the United States and mentions the vulnerabilities to high level companies in a technology conference based on the talk. Chris Roberts's plee for the updates and security issues should hopefully nudge all of the countries who are struggling to maintain integrity of safe data and cyber security on airplanes and other forms of transportation. Throughout the article most transportation industries are in denial of the state of the vulnerabilities. Chris states that even though these industries are in denial there is still a push from the US Departments of Homeland Security are worried about the performance of these sectors. This brings us to a problem with how data is maintained by companies which will use these new technologies inside of the vehicles we drive and luxury smart cars. In the next article Reneasas Electronics has revealed that they are connecting the more industrial giants inside of the IoT applications in smart vehicles. This now brings AWS and other large technologies such as Google and Greengrass to offer scalable open-source language based applications for its vehicle API in order to allow for weather tracking, conversation tracking and even behavioral analysis to the driver's vehicle all with or without the permission of the driver. Evertime you turn the key you are signing an unspoken contract to these service providers. This becomes even more frightening as the same company has open-source languages and data-sharing that are easily accessible to the vehicle through it's API interface. The final article exposes a lot of the vehicular vulnerabilities, elements common to daily tasks for drivers tools such as vehicle enabled wifi and telematics and bluetooth are all vulnerable systems and compromising them is very simple as most companies don't have a strategy to protect agains attacks to vehicle's ECU. Attacks to these ECU elements will destrory most of the boot systems and can be a problem as most of the system's will continue to face attacks unless companies take the time to fix the ECU on these data vehicles. The reason all of this is relevent is because there are an estimated 152 million vehicles that will feature connections to the internet and the likely hood of your data to be compromised at a red light with the right person next door could be come an increasingly harsh reality to tesla drivers with rolex watches and alot of interesting data to harvest.