The Security of Vehicles on the “Internet-of-Things” (Intro to series)

For most of its history, the automobile has been a narrowly purposed tool for transporting things and people from place to place, safely and reliably. Style and comfort were always important features; there was a radio to listen to, and in a bygone era you might use your car to watch a drive-in movie, but the functional repertoire of the automobile was rather limited.

All this has changed as the automobile has become an increasingly important participant in the internet-of-things(IOT). A modern vehicle is likely to be one of the most powerful and complex computing systems a consumer owns, running 50-100 million lines of embedded code and continuously communicating with both local and remote devices.

Internally, an automobile may have 80 electronic control units(ECU) communicating over a CAN bus. These include units for engine, powertrain, transmission, brakes, suspension, seat-control, auto and navigation.

Recalls and Updates

Embedded electronics gradually found their way into automotive design as passenger comfort features and specialized components such as fuel-injection systems. The electronic devices that replaced mechanical systems were relatively simple and air-gapped by virtue of their lack of sophistication and dearth of other devices with which to communicate. This made them “secure” in the networking sense and, as they provided similar or better performance and reliability to the mechanical systems they were replacing, the vehicle design was improved in every sense.

Consumer recalls of vehicles are slow and costly and require thousands(if not millions) of cars to be delivered to dealer service centers. The recalls are damaging to the reputation of the manufacturer, and often incomplete (it’s difficult to force a consumer to surrender their vehicle), leaving potentially dangerous vehicles on the road. Historically, even if a recall was due to, or could be repaired by altering the firmware in an embedded component (which becomes increasingly likely as more complexity is offloaded to embedded processors), the network isolation of the components kept the recall process cumbersome and expensive.

The landscape of automotive repair and maintenance changes completely as vehicles join the IOT. The Tesla Model S was the first mass production vehicle with embedded system firmware that could be completely updated over-the-air(OTA). Fixes which would have previously

required a traditional recall, could be done quickly (over wi-fi), quietly, thoroughly (nearly all vehicles are updated) and cheaply.

Embedded automotive systems are now routinely updated with fixes and enhancements that would have fallen below the threshold of seriousness for traditional recall.

The Importance of Security

The technology and innovation which is allowing vehicles to join smartphones as one of the most common participants in the IOT, has brought innumerable benefits in terms of safety, reliability and convenience. However, embedded systems designers must consider the implications, both positive and negative, of bringing the automobile into the world of tablets, laptops and smartphones.

Manufacturers will continue to respond to consumer expectations for more features, particularly those related to communication, navigation and entertainment. This will increase the number of ECUs, the complexity of the CAN bus and the number communication channels available to the vehicle. With this connectedness and complexity comes an increase in potential flaws and vulnerabilities.

If we consider of some of the unfortunate, but not-infrequent things that can occur when the security of a smartphone is compromised, juxtaposed with a computer controlled transmission, brakes and steering (not to mention ADAS), it becomes clear that security, as much as safety and reliability, should be a primary consideration in the design of an embedded automotive system architecture.

This is more than a hypothetical. The ability to remotely hack into a common model of Jeep Cherokee (as it drove on the highway) and take control of critical subsystems was clearly demonstrated in 2015.

A Series on Security

In this series we're going to examine network security as it applies to vehicles as they play a larger and more important role in the IOT. We'll examine how embedded systems for vehicles are currently designed, implemented and updated. We'll also looks at methods of attack and potential vulnerabilities along with best practices and ways of hardening critical subsystems.

Topics will include:

- Securing over-the-air updates
- Designing a secure system architecture
- Vehicle network anonymization