The Connected Car

by

Jay Wack, President CEO TecSec, INC

July 3, 2014

Introduction

Today's cars are so complex electronically that they're perhaps best thought of as mobile computer networks. The cars of tomorrow—which are already starting to appear today—will be increasingly connected—to the Internet, to each other, and to roadside wireless infrastructure.

Dedicated Short Range Communications (DSHC) Vehicles

The U.S. Department of Transportation (DOT) has designated IEEE 802.11p as the basis for Dedicated Short Range Communications (DSRC), by which a vehicle can communicate with other vehicles and roadside infrastructure. DSRC enables cooperative cruise control—cruising as part of a pack on the freeway—as well as collision avoidance, electronic road pricing and toll collection, electronic parking payment, and even braking for a red light that you may not have noticed. Beyond paying for tolls and parking, DSRC could turn your car into a 4-wheeled wallet, enabling you to drive through your favorite fast-food or coffee outlet without having to dig out your credit card.

In order to provide all the functionality in your car of your smart phone—including navigation, communication, multimedia, gaming, and location-based services ("Where's the nearest Italian restaurant?")—the average new car may have as much as a mile of wiring inside and contain over a hundred separate electronic control units (ECUs) that communicate over a variety of networks and buses. Add to that all the cool functionality that DSRC can enable and the system gets exceedingly complex.

The very complexity of in-vehicle infotainment (IVI) systems raise serious security issues, since you're connecting systems containing consumer-grade security with mission-critical systems that control the operation of the vehicle.

One weak point is the Controller Area Network (CAN) bus, over which the various ECUs communicate. While devices on the bus may be secure, the bus is not—which means the system as a whole is not. CAN is a message-based protocol with no built-in security features.

A couple of years ago the Center for Automotive Embedded Systems Security (CAESS) demonstrated the fragility of the underlying system structure. They connected a packet sniffer to the On-Board Diagnostics II (OBD-II) port to analyze CAN bus traffic. Using a wireless link they were then able to use that information to start and stop the car, race the engine, lock individual brakes, unlock the doors, and pretty much control the entire car.

Taking their hacking to the next level the CAESS team was then able to take over control of a vehicle remotely through its telematics system. They demonstrated that it's possible to hack a car with malware inserted into an MP3 player or transmitted over a Wi-Fi connection. Devices relying on an 802.11p wireless connection may be particularly vulnerable.

When you're mixing consumer-grade applications and you want security, you're always going to have maliciousness or just software that doesn't work the way it's supposed to, however, this is not just a matter of security; there is also privacy to consider. As pointed out above, the broad connectivity of cars potentially gives manufacturers access to data we may consider to be private, whether that's our music and navigation data or more personally, our location, family information and potentially other sensitive information. So the physical loss of the car could in fact be coupled with the loss of personal privacy.

The Constructive Key Management (CKM) technology addresses both the need for controlled connectivity as well as the constraint of content access and use. The CKM process creates cryptographically protected smart objects, which means the data objects can be protected persistently, regardless of the method of transmission and storage. This approach means the open communications bus found in the CAN standard can be used safely and with precision. The right data and sensor are cryptographically separate from all other data/sensor pairs. Data can be created or consumed by a given function with confidence that it will only be accessed by the appropriate/agreed to relationship. More broadly, the use of the CKM attribute based access control process can enforce data context usage, providing the mechanism to make decisions about data based on; the type of data the collection method, the owner of the data. And further, within those groupings, the data is protected throughout its life; from point of generation, through transmission, collection, use, storage, and archive, until destruction.