Visteon®

NEWS RELEASE

A conversation with cybersecurity expert Srini Adiraju

2017-08-25

With increased connectivity comes an increased risk of cyber security attacks – and with the auto industry having experienced several highly publicized system hacks, Visteon is addressing cyber security at the core of its technology development. To ensure that security is designed into all products and processes, a team of cyber security experts – with experience across a range of industries – is working with the company's technology and product development centers to cyber-secure future technology.

Srini Adiraju, cyber security expert, joined Visteon in early 2016, specializing in advanced technology development, with a background in software development for realtime products and systems software, mainly in the casino and gaming industry. Here, he shares his insights on cyber security within the auto industry.

Q. What is driving the heightened focus on cyber security in the auto industry?

A. When cars were not connected to the internet, physical access to the vehicle was required to impact its safety or performance. That's no longer the case; the new automotive landscape is more electronic and more connected. That means a simple small, open "door" is enough to get in and initiate a security threat remotely, as the industry has seen in several highly publicized incidents.

Q. What does the term cyber security mean to you?

A. Cyber security is not a software asset; it is a foundation. It is not something you can see or feel. Not everything related to cyber security is a technical solution; it's a combination of technology solutions, manufacturing and development processes. It's really about ensuring a product is secure from start to finish, especially in the connected car – and ultimately – the autonomous vehicle.

Q. You come from a security background in the (casino) gaming industry. What similarities exist between the gaming and automotive industries?

A. There are many parallels. The software architectures are similar. In the gaming world, you have multiple displays, consisting of hardware similar to an automotive head unit. In the last decade, slot machines moved from stand-alone machines to networked machines – so network security is very important for every device today. During that period, the gaming industry deployed new security measures such as secure boot (a security technique that helps ensure a device boots using only trusted software), secure communications and secure storage. These are all pertinent to automotive today. Also, the gaming industry has many regulatory requirements, as does automotive.

Q. Which products require the most attention to cyber security?

A. Most of the highly publicized "hacks" of vehicles occurred through the telecommunications control unit (TCU) that is connected to the internet. Any device that sets up a pipe to the internet is more susceptible to hackers. Since all ECUs are connected through a CAN network, one weak link or "open door" can make other ECUs susceptible to these attacks, either through the network, USB or onboard diagnostics (OBD) II port.

Q. What is Visteon's approach to vehicle security?

A. We are taking a very pragmatic approach. We should protect what we know and constantly monitor what we don't know. One of our key pillars is a secure boot – ensuring that only very trusted software inside the ECU is being used and protected. Second is secure communications – if you are connected to the internet, we must make sure the communication is secure. The third pillar is secure storage of customer and vehicle data. The fourth pillar is secure software updates.

We are working to deploy the SAE cyber security standard, J3061. One of the key foundations of J3061 is "secure development life cycle," which aims to improve the hardware and software security through groundup design.

With a security focus at every level, the quality of our software will rise to new levels. For example, when writing software, we make sure we are validating all inputs and outputs and using thread-safe, secure application programming interfaces (APIs). Security will be a focus at every stage of product development – from conception to end.