SECMATION

Autonomous Vehicle Cybersecurity

Hal Aldridge, Ph.D., CEO
hal@secmation.com

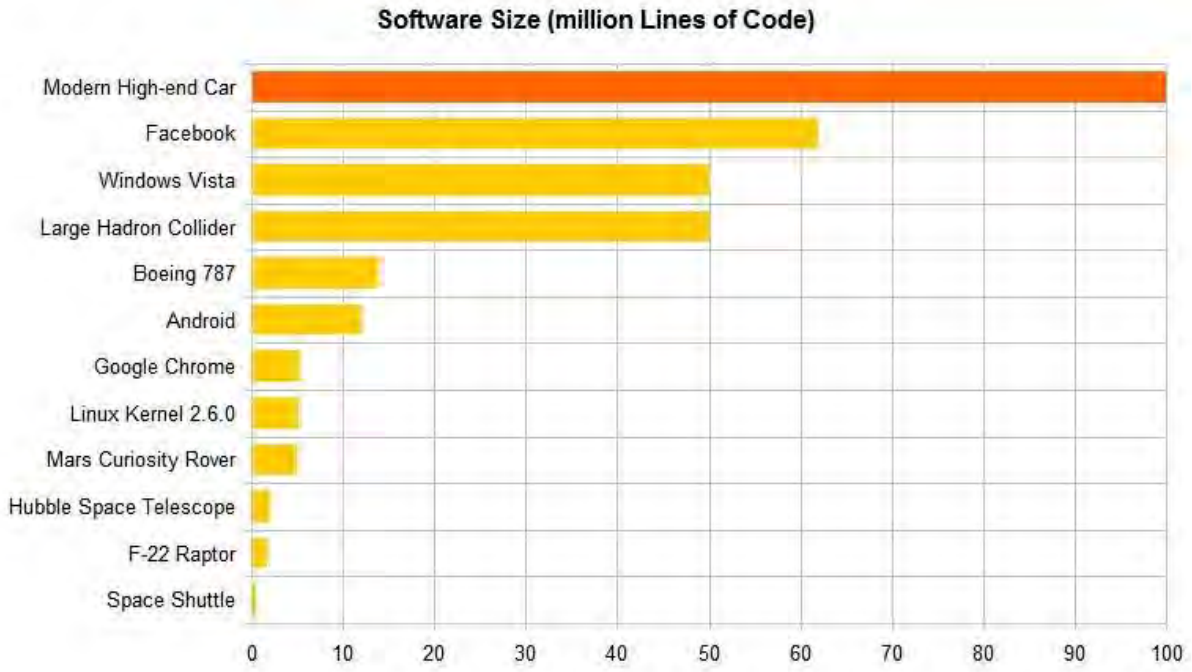
Background

Secmation is a growing business located Raleigh, NC, specializing in Cybersecurity R&D and Product Development in cybersecure applications for uncrewed and autonomous systems.

We’re Hiring New Grads and Interns
www.secmation.com

SECMATION

“This Car Runs on Code”

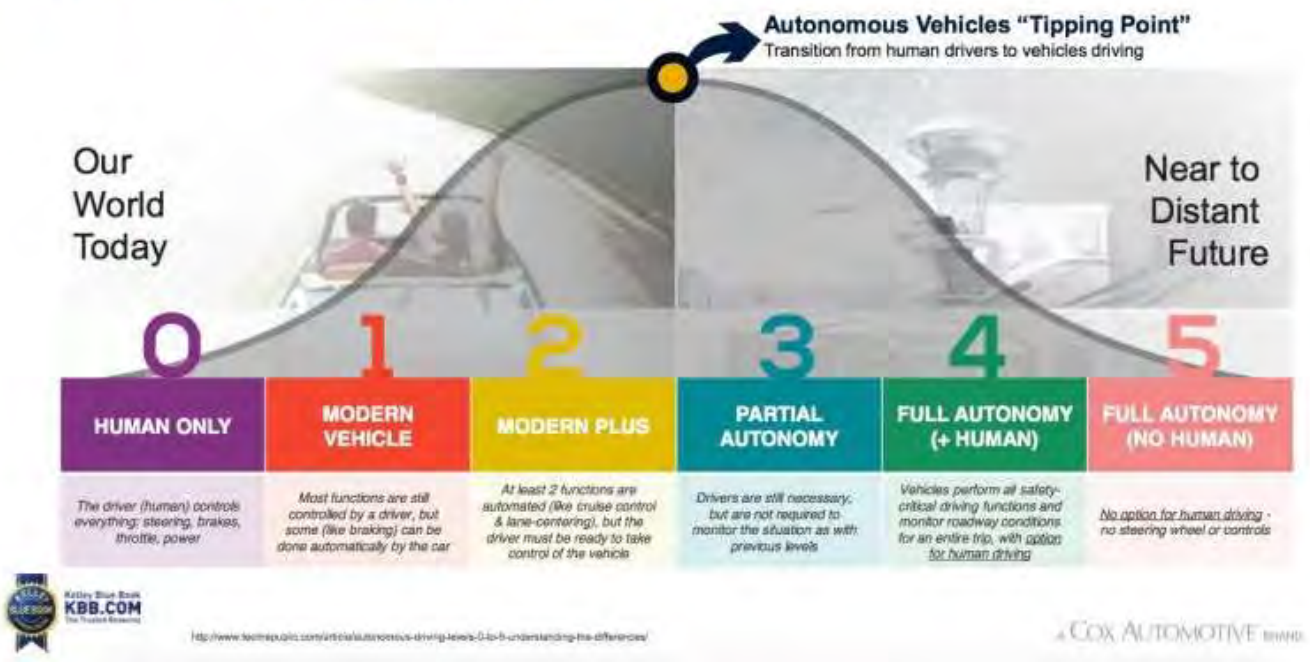


- Current automobiles have ~100M lines of code
- That is before all the “real” self driving features are added in the future
- Will be increasing to 200-300M lines of code near term
- Code comes from multiple vendors the automaker must integrate and ensure they function correctly
- ***But what about cybersecurity?***

SECMATION

Self Driving Levels

The levels of Autonomous Vehicles



- We have a long way to go to get to "full self driving" in any environment or condition
- All applications you see now (e.g., robot taxis) all are in constrained/limited environments with $$$ sensor systems
- There is a much shorter path to develop attacks to disrupt it….
- ***…and not enough attention on preventing attacks until "something bad happens"***

SECMATION

Modern Car Vulnerabilities

DARKReading | The Edge | DR Tech | Sections | Events

ICS/OT Security | 5 MIN READ | NEWS

From Ferrari to Ford, Cybersecurity Bugs Plague Automotive Safety

Security vulnerabilities plague automakers, and as vehicles become more connected, a more proactive stance on cybersecurity will be required — alongside regulations.

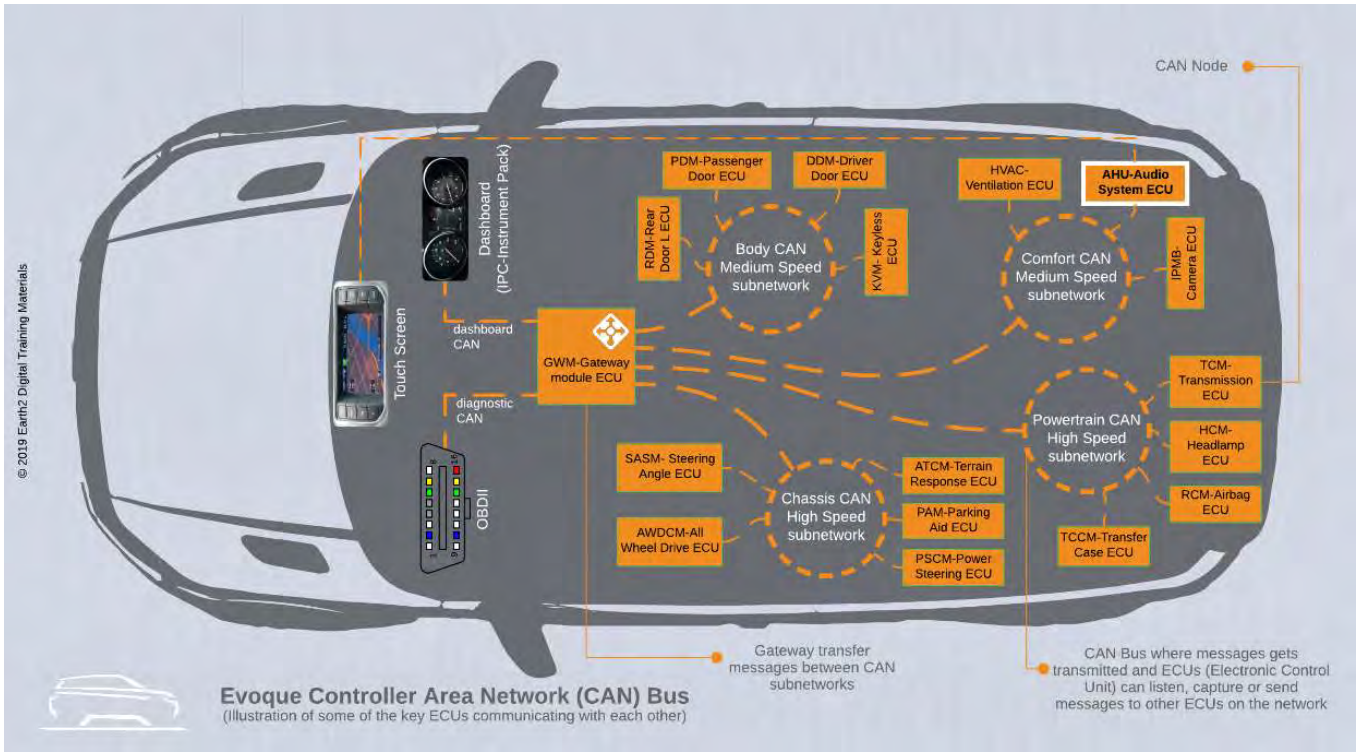
Nathan Eddy
Contributing Writer, Dark Reading
January 06, 2023

Source: Christopher Vincenti via Alamy Stock Photo

- A quick Google search brings up the current state of automotive cybersecurity. Not ideal, but better than a few years ago.
- Example of known vulnerabilities from https://samcurry.net/web-hackers-vs-the-auto-industry/
- Hyundai/Genesis
  - Fully remote lock, unlock, engine start, engine stop, precision locate, flash headlights, and honk vehicles using only the victim email address
  - Fully remote account takeover and PII disclosure via victim email address (name, phone number, email address, physical address)
  - Ability to lock users out of remotely managing their vehicle, change ownership

SECMATION

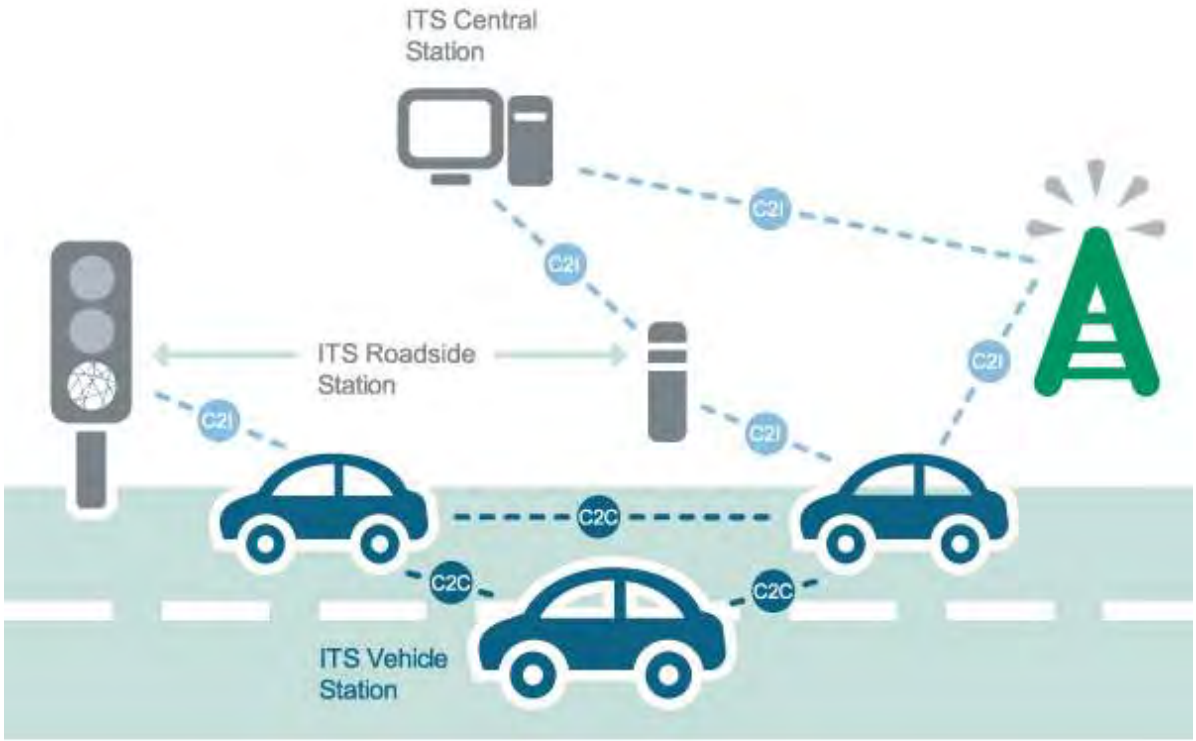
Modern Car Vulnerabilities



- CANBus is the industry standard for vehicle communications
- ***CANBus is not encrypted or authenticated***
- Presents an easy entry point for direct vehicle access or remote access through a compromised Electronic Control Unit (ECU)

SECMATION

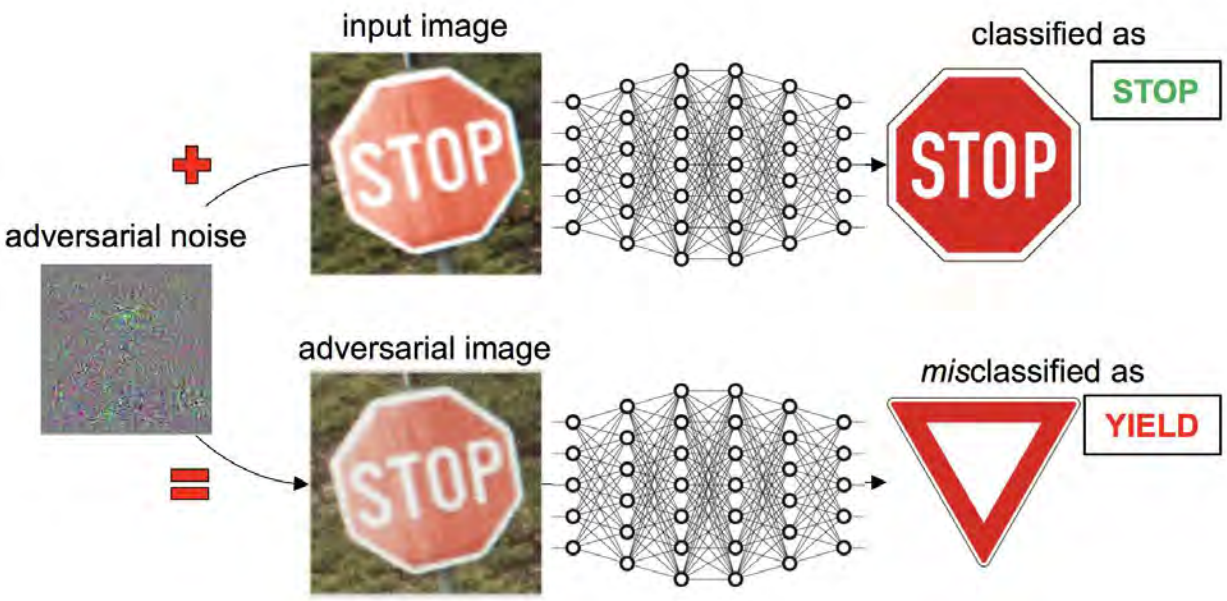
Vehicle to Vehicle Comms (V2V)



- A key element of the future of autonomous vehicles is communications
- An autonomous vehicle would not rely solely on its onboard intelligence/sensors
- The vehicle would get real-time data form multiple sources **INCLUDING** other neighboring cars
- ***Opens many different attack vectors that do not currently exist***

SECMATION

AI/Machine Learning



- Only being deployed now
- Will be a key part of future autonomous vehicle solutions
- Presents a new area of research in vulnerability analysis, attack design, and cybersecurity

SECMATION

What Are Some Solutions?

- Establish cybersecurity standards for the automotive industry
  - Defines “best practices” which can eliminate many simple vulnerabilities
  - ***Provides mechanism for certification/compliance. Think like getting a “Crash Test Report” for the cybersecurity of a car you are planning to purchase***
- Better access to SW updates/patches
- Understanding you cannot have safety without cybersecurity.
  - **Active protection systems are SW based**
- Software Bill of Materials (SBOM) – Manufacturers must fully understand all vehicle SW supply chain and pedigree
- ***Different mindset – An automobile is a safety critical network of computers with wheels and must be treated as such***

SAE and ISO Publish Joint Automotive Cybersecurity Standard

2021-09-03 WARRENDALE, PA.

Standard is Supported by SAE's New Cybersecurity Training Program and Webcast

WARRENDALE, Pa. (September 3, 2021) – SAE International, in collaboration with the International Organization for Standardization (ISO), announced today the publishing of ISO/SAE 21434™ Standard: Road Vehicles – Cybersecurity Engineering. The standard helps the industry define a structured process to ensure cybersecurity is incorporated into the design of road vehicles, including systems, components software and connections of any external device or network.

SECMATION

SECMATION

We’re Hiring New Grads and Interns
www.secmation.com