Topics in Computer Science: Security Challenges in Connected and Autonomous Vehicles

Gavan Phitides, Umair Oad

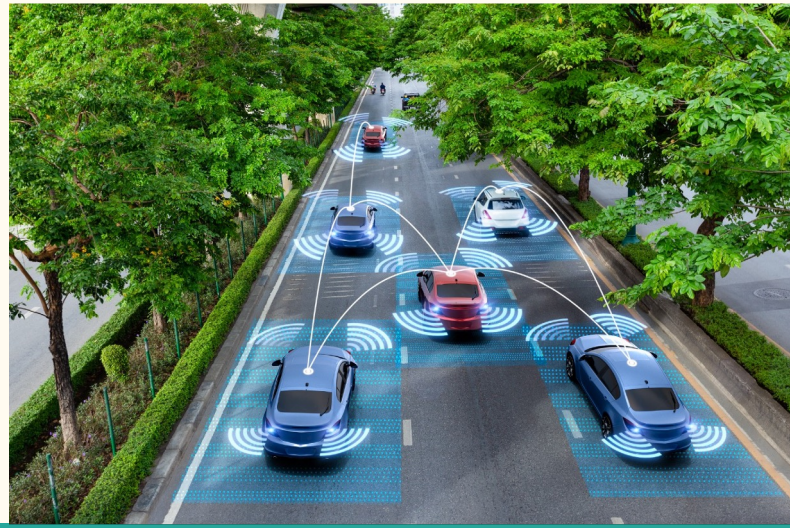
What is CAV?

- CAV: Connected and Autonomous Vehicles
- Connectivity
  - Share data with other entities via a multitude of methods
  - Entities can range from a variety of possibilities

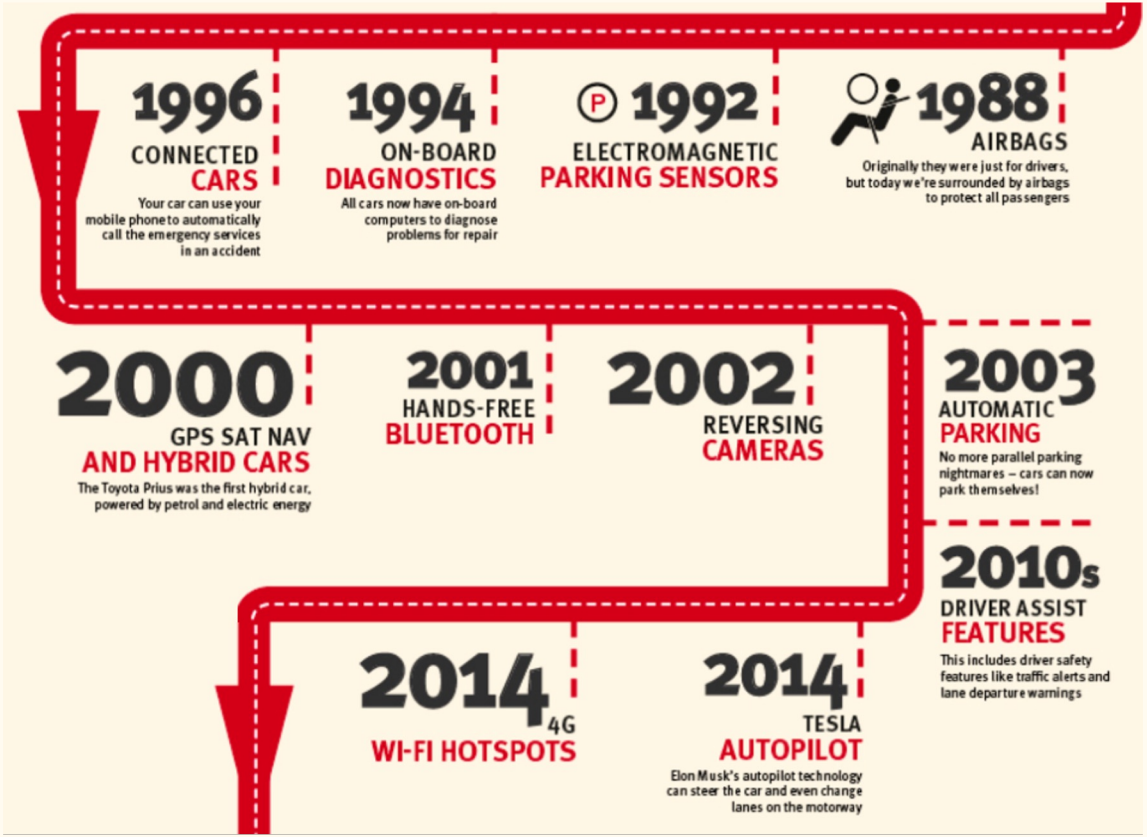
- Automation
  - Automatically handling part or whole of the driver's task
  - Advanced Driver Assistance Systems are in play in modern vehicles
    - AEB: Autonomous Emergency Braking
    - LKA: Lane Keep Assist
    - ISA: Intelligent Speed Assistance

What is CAV? Continued

- Goals at hand:
  - Promote driver safety
  - Reduce collision/accident rates
    - 42,915 deaths in 2021
    - 10.5% increase from previous year, 38,824 deaths
  - Clear traffic congestion
  - Lower pollution



Timeline of Connected Vehicle Functions



Modern Vehicle Functions

We can group modern vehicular functions into categories:

- Vehicle to occupant (V2O):
  - Bluetooth for wireless devices
  - UWB phone-as-a-key
- Vehicle to vulnerable road users (V2VRU):
  - Pedestrian detection
  - Recognizing motions
  - Warning before a crash
- Vehicle to vehicle (V2V):
  - Lane change warnings
  - Blind spot warnings
  - Self-organized autonomy

Modern Vehicle Functions Continued

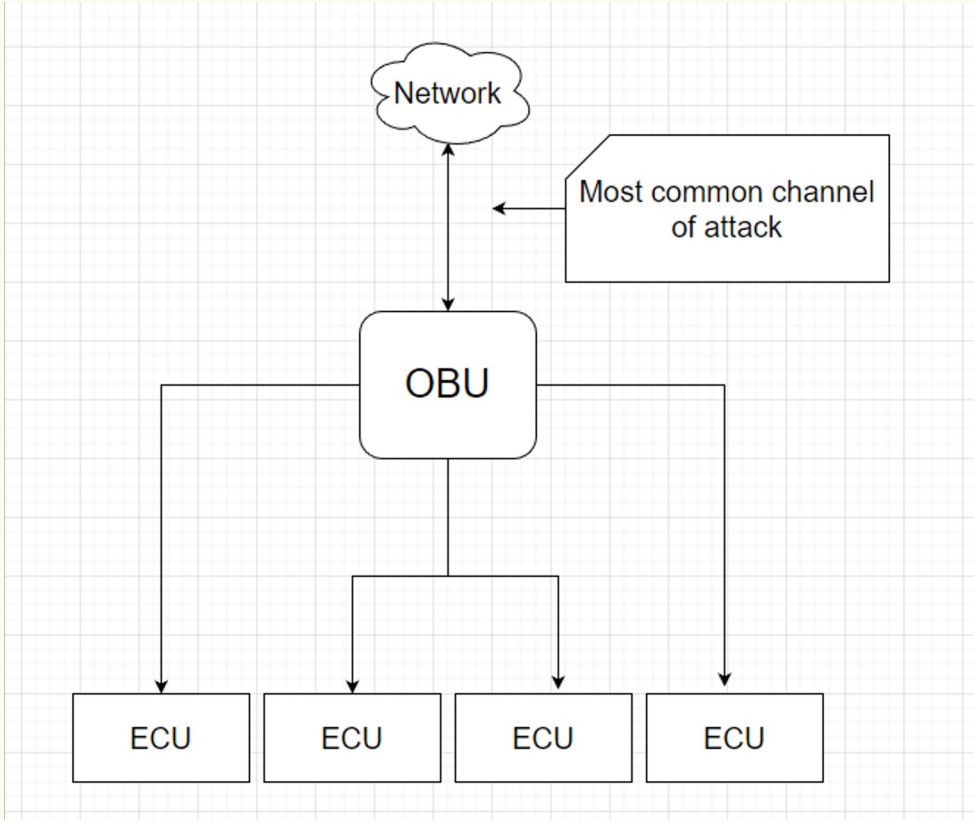
- Vehicle to environment (V2E):
  - Risk prediction when driving
  - Road condition monitoring

- Vehicle to infrastructure (V2I):
  - SOS services
  - Do-not-pass-warning
  - Preemptive emergency vehicle signal detection

Understanding Connected Vehicles

- CV -(Connected vehicle)
- CV Network
  - System of IoT devices in CV system
- OBU (On Board Unit)
  - Speaks to network and ECUs
- ECU (Electric Control Unit)
  - Controls functions of vehicle

V2X communication flow chart



Attack Vectors on connected vehicles

- External threats can come from both wired and wireless sources
- 3G/4G/5G and wifi attacks can come from mobile devices, access points
- Radio frequency attacks can come from smart keys
- Wired attacks can come from items such as flash drives and connected diagnostics tools
- Wired Attacks are typically of less concern

Tangential Attack Vectors on connected vehicles

- CVCS (Connected Vehicle Charging Stations)
- Charging stations network
- Do you think the an attack on the charging station network could affect more than just connected vehicles?

Types of Attacks on CVCS

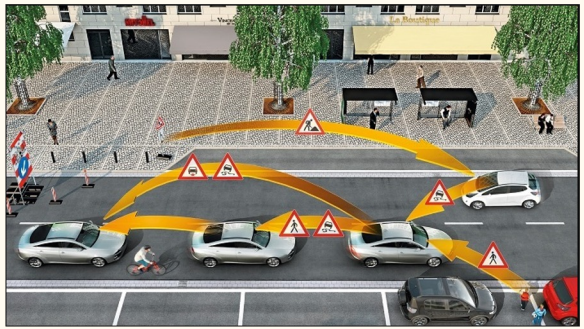
- Physical: CVCS lacks physical security, can damage charging units, steal electricity, or install malware through usb or other ports.
- Local: exploit based on gaining logical access to CVCS through firmware vulnerabilities.
- Limited Remote: Attackers can take advantage of weak credentials or outdated encryption of Local Area Networks near CVCS to find entry points into the system.
- Fully Remote: CV management systems through online portals or mobile apps. Over The Air updates to the CV, the management system or the CVCS all leave potential entry points for malicious activity.

Typical Methods of Attack

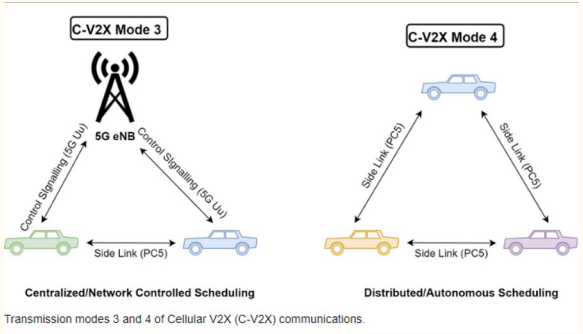
- SQL Injections: allows the attacker to have access to privileged user information and manipulate firmware.
- XML injection: allows the attacker to inject HTTP requests in the system and sometimes gain remote access to the CVCS.
- Server-Side Request Forgery(SSRF) Allows an attacker to redirect traffic towards internal and external endpoints in order to cause DDos as well as being able to read files and record logs of the CVCS.
- Cross site scripting(XSS): Allow the attacker to hijack user accounts and sometimes even admin accounts
- Hard Coded Credentials: While it makes the job easier for Software engineers, but it allows attackers to recover the login credentials in the source code or associated apps in order to gain unauthorized access to CVCS

Channels of Attack

DSRC - Dedicated short-range communications, are one-way or two-way short-range to medium-range wireless communication channels specifically designed for automotive use.



C-V2X Cellular Vehicle to environment, a 3GPP standard for V2X applications such as self-driving cars. It is an alternative to 802.11p, the IEEE specified standard for V2V and other forms of V2X communications.



Transmission modes 3 and 4 of Cellular V2X (C-V2X) communications.

Attacks on CV IoT Systems

- Confidentiality - Attackers can eavesdrop on DSRC or C-V2X channels
- Integrity - Attacker could replay or manipulate messages to feed false information
- Accountability - Attacker can manipulate how your vehicle is perceived by the network
- Availability- The availability of the system is attacked if the units are used in a part of DDOS attacks.
- Authenticity - Attackers can manipulate certification of the data bases

How to identify a Compromised Vehicle

- V2X can have channel security but little way of being able to understand what types of messages are valid to execute logically and what is not. A compromised machine could cause accidents without the vehicle ever knowing its information was dangerous.

- Cryptography can be used to generate signature that verify authenticity of commands, but this only applies to uncompromised devices. Once a device is sufficiently compromised cryptography is no longer enough to protect against cyber havoc.

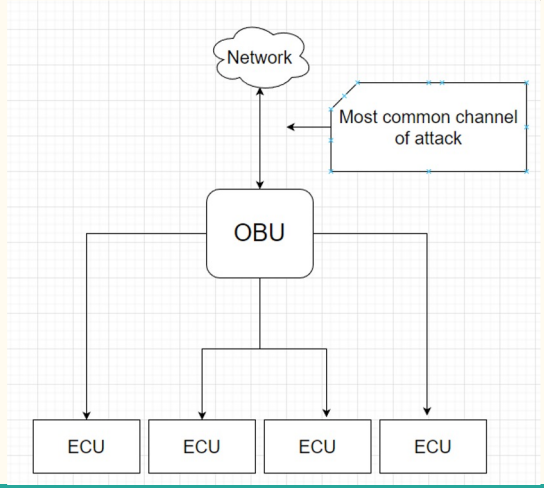
- This is addressed this by DCI(deep content inspection) and misbehavior detection

- Validate the plausibility of information by checking other systems to see if the command is reasonable to execute.

Logical detection of malicious messages

- Sentinel-V2X - A system in the OBU is a system that inspects messages for malicious messages using intrusion detection and prevention systems

- Must check both incoming messages and outgoing messages from the CAN Bus to the OBU, and from the OBU to other devices in the network



Plausibility Checks

Metrics of plausibility:

- Range of message
- Location plausibility
- Sufficient speed of message
- Position consistency between two messages
- Frequency of message beacon is compliant with standards
- No suddenly appearing messages

Addressing a Compromised CV

- The certificate of the vehicle is revoked and it is no longer able to communicate with other vehicles or units. This happens in stages.
  - Warning messages
  - Begin to deduct the plausibility score
  - Begin to revoke communication privileges
  - Fully revoked certificate and remove compromised vehicle from the system

- The information gathered by the addressing of the attack is used to develop better more effective ways of preventing them in the future.

- The better the vehicles system is built to withstand theses attacks in the first place the better

The 2015 Jeep Hack

- Charlie Miller and Chris Valasek discovered security vulnerability in Jeeps
- Requires vehicle's IP address, general location and VIN, or Sprint connection
- Hacked a Jeep in 2015 on the highway
- Turned on wipers, increased radio volume drastically, and killed the engine to halt the car completely
- Caused a recall of 1.4 million vehicles by Chrysler
- Hackers were "white hat" hackers; they did this with the intention of filling in security holes

General Concluding Points

- Connected vehicles are most vulnerable to wireless attacks
- In order to address this vulnerability, we must have several tiers of protection to verifying the messages are not compromised
- The solutions must work in tandem with logical algorithms to determine validity and reasonability of messages communicated in the network
- The best way for this to be addressed is to learn from current modes of attack and continue to make better security solutions from the design of the car instead of after release

QnA Session

- Feel free to ask any questions that come to mind!
- Share thoughts that you might have had during the session!

Works Cited

Abdelkader, G., Elgazzar, K., & Khamis, A. (2021, November 19). Connected vehicles: Technology review, State of the art, challenges and opportunities. MDPI. Retrieved October 17, 2022, from https://www.mdpi.com/1424-8220/21/22/7712

Adamu, H. (2022, May 19). Samsung's UWB-based digital car key arrives on the genesis GV60 electric. Android Police. Retrieved October 17, 2022, from https://www.androidpolice.com/samsungs-uwb-digital-car-key-genesis-gv60-electric/

Bmw. (2021, December 14). Connected car. . Retrieved October 17, 2022, from https://www.bmw.com/en/innovation/connected-car.html#:~:text=Connected%20cars%20with%20an%20emergency,in%20a%20phone%20call%2C%20though.

Connected and autonomous vehicles. Brake. (n.d.). Retrieved October 24, 2022, from https://www.brake.org.uk/get-involved/take-action/mybrake/knowledge-centre/vehicles/connected-and-autonomous-vehicles#:~:text=Connected%20and%20autonomous%20vehicles%20(or%20CAVs)%20combine%20connectivity%20and%20automated,capabilities%3B%20GPS%20and%20telecommunications%20systems.

Erwin, B. (2022, July 26). *The groundbreaking 2015 Jeep hack changed Automotive Cybersecurity*. Fractional CISO - Virtual CISO. Retrieved October 17, 2022, from https://fractionalciso.com/the-groundbreaking-2015-jeep-hack-changed-automotive-cybersecurity/

Jardinemotorsuk. (n.d.). The history of Car Technology. Driving Seat. Retrieved October 17, 2022, from https://news.jardinemotors.co.uk/lifestyle/the-history-of-car-technology

Vehicle Safety Technology. Brake. (n.d.). Retrieved October 24, 2022, from https://www.brake.org.uk/get-involved/take-action/mybrake/knowledge-centre/vehicles/vehicle-safety-technology