Cooperative Systems R&D
Southwest Research Institute
IVS.SwRI.ORG

Safety Impacts of Connected and Automated Vehicles

Paul A. Avery
Principal Engineer – Cooperative Systems
Southwest Research Institute
+1.210.522.6732
pavery@swri.org
Connected Vehicles Communication

However!

Special Applications Like Platooning
Connected Vehicle Demonstrations
Wrong Way Driver Detection and Alert

**LEGEND**

1. Region monitored for wrong way driver detection
2. Roadside equipment monitors BSMs and detects wrong way driver
3. Wrong way driver alerts generated via Infrastructure to Vehicle and approaching vehicles are alerted
4. TMC operator and responders are notified of wrong way driver
A roadside monitoring system detects an over-height commercial vehicle and sends the following info to the truck:
- over-height warning
- exit ahead with route info
- disablement / vehicle limiting region

This will need to be a directed message to the truck that violated the sensor and not broadcast to all vehicles. To do this, the monitoring system could leverage BSMs received at the time of the violation from the sensor region and send a directed message to that vehicle.

The commercial vehicle does not take the exit and enters the Disablement / Vehicle Limiting Region. OBE acts appropriately to disable or limit the vehicle.

Vehicle is disabled or speed limited prior to hitting the bridge.

The commercial vehicle takes the exit and the driver is provided alternate route info.
V2V – Blind Spot Warning
A monitoring system will be integrated with existing railroad grade crossing warning equipment that would begin emitting the SAE 2735 Roadside Alert message once activated and stop when deactivated. The vehicle would process the Roadside Alert message and determine if the direction/ location/ extent is appropriate (e.g. trucks traveling away from the crossing that receive the message would not display the warning).
What About Evacuations?
Event modeling

- Vehicles react to event information by altering their route choice

Road volumes after event notification – 50% CV enabled
Ooops…. We Forgot About Security

(CNN) -- When car companies begin exhibiting at mobile shows, it's a sign that the "connected" vehicle has truly entered our lives. It's as if we're allowing the car to drive itself, by allowing us to take our digital lives with us as we hit the road.

But while Ford's unveiling of its latest car at Mobile World Congress -- a major mobile phone industry event -- this week may have new automotive age, it also heightens fears that our tech-savvy cars could be hijacked by hackers.

Just like our phones and smartphones, the computerized cars that have infiltrated almost every aspect of modern vehicles can be just the type of device that hackers could use to their advantage. They have to be aware of the potential consequences.

Car-hacking: Remote access and other security issues

It's not time for full-on panic, but researchers have already identified this problem. In a recent study, they found that some cars were vulnerable to hacking attacks.

The study, conducted by the University of California-San Diego, found that remote access was a significant concern. They found that hackers could control the car's functions remotely, such as opening the doors or starting the car.

A 2011 report by researchers at the University of California-San Diego and others note numerous "attack vectors," including mechanical tools, CD players, Bluetooth and cellular radio, among the potential problems in today's computerized cars.

Computerworld: A disgruntled former employee of Texas' flatlander Caddo County chose a creative way to get back at the Austin-based company. He breached the company's computers and remotely activated the immobilization system, which triggered the horn and disable the car in more than 100 of the vehicles. The dealership maintained a system in their cars as a way to deal with customers who default on payments.

Police arrested the man and charged him with breach of computer security. His legal status was unclear as of our deadline for this story.

Out-of-control honking horns may be annoying, but other types of hacking, such as cutting the engine of unsuspecting drivers, could have deadly consequences. Although most experts agree there isn't an immediate risk, vehicle hacking is something that bears watching.

Exclusive: CEO says hackers tried to extort data, money

Kariem Hijazi knew his nightmare was just beginning when he saw that a mysterious e-mail had arrived in his inbox at 3 a.m. on May 26 that included his e-mail password and the subject line "Let us talk.

That would mark the beginning of a weeklong saga of e-mail exchanges and Internet Relay Chat (IRC) discussions in which Hijazi says a group of hackers told him they would publicly divulge information they had gleaned from snooping on his accounts if he revealed sensitive security information acquired by the botnet tracking firm. Untraceable, that he launched last year. The hackers, who call themselves LulSec, wanted to know the whereabouts of compromised computers on the Internet that when remotely controlled are used en masse to attack Web sites, he told CNET in an exclusive phone interview last night.

When he refused, LulSec went public with his data. Hijazi says, posting his personal contact information, e-mails, and chat logs for download online yesterday as part of a campaign to embarrass the FBI and its InfoGuard partner. The group had hacked the Web site of InfoGuard Atlanta and grabbed usernames and passwords for about 100 members, including Hijazi.

Because Hijazi had used the same password on the InfoGuard site that he used on his personal Gmail account and his corporate Google Apps account, the hackers were easily able to spy on his personal and business activities.

Hijazi contacted the FBI right after that first LulSec e-mail and said he plans to prosecute if he can.

"They had me under the gun for a little over a week with threats and extortion," says Hijazi, chief executive of Untraceable. "The very nature of having to contend with someone who is holding something ransom is not pleasant!"
How The Nissan Leaf Can Be Hacked Via Web Browser From Anywhere In The World

Jason Torchinsky
2/24/16 2:10pm - Filed to: CAR HACKING

Even if you don’t understand the code, here’s what all that means: we have the ability to get personal data and control functions of the car from pretty much anywhere with a web connection, as long as you know the target car’s VIN.
Challenges with Connected/Automated Vehicles

**Recent Attacks:**
- Jeep Cherokee: “Hackers Remotely Kill a Jeep on the Highway—With Me in It”
- GM OnStar: “This Gadget Hacks GM Cars to Locate, Unlock, and Start Them”
- Tesla Model S: “Researchers Hacked a Model S… But Tesla’s Already Released a Patch”!

**Impact of these attacks:**
- Erodes public trust
- Raises awareness – improves security practices

Image Source: Wired Magazine
Detecting Global Misbehavior in a CV System

- False message inserted into CV system
  - Stalled vehicle
  - BSM showing velocity = 0mph
  - Emergency Braking
  - Wrong-way Driver, etc…
- CV-equipped vehicle(s) receive message and vehicle’s autonomy software or advanced driver assistance system (ADAS) system reacts
  - Hard braking
  - Swerving
- Causes secondary reactions from nearby vehicles
Automated Vehicles
Future of Traffic Enforcement?

“Does your car have any idea why my car pulled it over?”
Google teaches its self-driving cars to honk

Waterloo Region Record
By Marco della Cava

SAN FRANCISCO — Google’s self-driving cars are getting some attitude.

Company engineers have been working on teaching their autonomous vehicles the subtle — and often obnoxious — art of honking, according to Google’s May self-driving car report.

The innovation makes sense. After all, while Google’s 24 self-driving Lexus SUV fleet are hybrid machines with a modicum of engine noise, Google’s growing gaggle of 34 pod-like prototypes are all-electric machines that barely whisper their presence. Sometimes, a short stab of the horn is required to let folks know they’re coming.
Maybe Releasing Autopilot Into the Wild Wasn’t A Great Idea?
So How Do We Avoid This?
Connected-Automated Vehicles

(But Only If The System Is Cooperative)
Vehicle Platooning

• Rules must be established for joining a team: Max/min speed, following distance, vehicle performance/efficiency characteristics, etc
• Special message must be used, including a “Team ID” to enable cooperation among specific vehicles
Connected Vehicle Demonstrations
Wrong Way Driver Detection and Alert

**LEGEND**
1. Region monitored for wrong way driver detection
2. Roadside equipment monitors BSMs and detects wrong way driver
3. Wrong way driver alerts generated via infrastructure to Vehicle and approaching vehicles are alerted
4. TMC operator and responders are notified of wrong way driver

**Autonomous safe stop**

1. Region monitored for wrong way driver detection
2. Roadside equipment monitors BSMs and detects wrong way driver
3. Wrong way driver alerts generated via infrastructure to Vehicle and approaching vehicles are alerted
4. TMC operator and responders are notified of wrong way driver

Traffic Management Center

Vehicle Generates BSMs

Wrong Way Driver

No Message

Wrong Way Driver Ahead!

WARNING Wrong Way!
**Cooperative Vehicle-Infrastructure Situational Awareness**

High-Traffic Intersections, Work Zone & School Zones

**LEGEND**

1. Static situational awareness system detects pedestrians, bicyclists, & vehicles
2. Static system transmits situational awareness message & SPAT/MAP to surrounding vehicles
3. Vehicles contribute to the collective model of the area
4. Applicable for dangerous intersections, school zones, and construction work zones
Enhancing Work Zone Safety
Mobile Roadway Maintenance

**Legend**

1. Automated crash cushion vehicle follows lead maintenance vehicle
2. Automated vehicle monitors other vehicles to predict impending collisions
3. Traffic Management Center uses vehicle to infrastructure communication to monitor stationary work zone
4. Traffic management center implements rolling event response plan
5. Upstream vehicle receives advisory message regarding the mobile maintenance fleet
Cooperative Sensor Sharing for Unmanned Systems

- Developed under SwRI IR&D program Mobile Autonomous Robotics Technology Initiative (MARTI)
- Cooperative vehicle behaviors for sharing sensor data in a dynamic traffic environment
- Utilizes the sensing capabilities of other vehicles as extension of perception system

**Use-case: Pedestrian safety**

- Communicates V2V regarding position, speed, and heading of pedestrians at intersections
- Receiving vehicle determines appropriate action
Cooperative Vehicle Lane-level Model Generation Using DSRC

- Vehicles broadcast message on their location (Basic Safety Message)
- Roadside device collects messages for processing
- Using learning algorithms, the noisy data is reduced to lane-level GPS coordinates
- Data is reduced to minimum required set, and then re-broadcast to vehicles
- If obstruction is removed, vehicles will begin traversing the area again, and a new map will be processed and re-broadcast
Cooperative Systems R&D
Southwest Research Institute

Thank You