**EMCS2010: Applied Cryptography and Data Privacy**

Assignment: Connected Vehicle Technology and Privacy

Brian Russel Davis, [brian\_davis@brown.edu](mailto:brian_davis@brown.edu)

#### Introduction

Vehicle to Vehicle Communication has been proposed as a rule by the U.S. Department of Transportation. Citing an article from 2016 the “Proposed rule would mandate vehicle-to-vehicle (V2V) communication on light vehicles, allowing cars to 'talk' to each other to avoid crashes.” I have a nickname the proposal the iRobot Rule, because in the 2004 Will Smith movie nobody drives and the cars communicate with one another, for the safety of the occupants much like the proposed rule. I think the rule and V2V is an interesting proposition and I think there are ways to implement it without sacrificing privacy if we think through the needs carefully instead of focusing on the technology.

#### The Need: Safety from Collisions

Drivers on the roads have many needs, but there is none more important than the need to not crash into one another. This is presently handled now with the implementation of education and rules. Every driver is required to be licensed, the process of getting a license involves education and then when drivers are on the road they compelled by the law ( and the risk of harm ) to follow the rules. One could argue that not everyone follows the rules. I would argue no one does. Yet, we all get in vehicles on a daily basis. Our communication with our drivers and vehicles is mostly visual. We can “see” how far away they are from us when they are getting too close when they are slowing down. We use this data, our sight, to make intelligent decisions about what to do. All things being equal these in the moment decisions are pretty complex, and we take the complexity for granted because they are work of an organic supercomputer, the human brain. This is why the V2V communication seems simple on the face, but when one realizes what would have to be replaced in order for it to work the problems become more evident.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Driving Danger | Human Perception | Human Response | Computer Perception  Sensors Required: Video, IR, Ultrasonic | Computer Response |
| Front End Collision ( Driver runs into the car ahead ) | The driver perceives the car ahead is getting to close based on relative speed. | Slow down, *“I am going too fast”*. Change lanes, *“They are going too slow.”* Braking is dependent on relative speed, drivers on all sides, behavior(s) of other drivers in the last 30 seconds. | There is an object ahead that is a danger based on the current velocity and relative distance. | Alert the driver. Activate Braking? |
| Back End Collision ( Driver is hit from behind ) | The driver perceives the car behind is following too close based on relative speed. | Speed Up, to create more room. Change lanes, to allow the other driver to pass. | There is an object behind that is a danger based on the current velocity and relative distance. | Alert the driver. Increase speed? |
| Side Collision ( Driver is hit from the side ) | The driver perceives that the car on the side is unaware of their presence. | **Honk**, alert the other driver of your presence. **Slow down**, let the other driver ahead of you. **Speed ahead** of the driver. | There is an object on that side that is a danger based on the current velocity and relative distance. | Alert the driver, then what? |

#### Communication: What would make V2V Effective

Based on the table above we can make some further assumptions above the type, speed and frequency of communication need to mimic human perception/response and improve it. In order to V2V to work it needs more than just positioning data, it also needs video data, audio data, real-time weather data and data about the rules that govern the specific piece of roadway the driver(s) are in. V2V systems don’t need to just share the data, they will also need to have a common language to share information about things like object recognition, for example. If there is a mattress sliding down the freeway, this should be handled differently than a car that is suddenly braking. All of this data is not just heavy, but there would be a lot of it. Terabytes of data could be generated in less than a minute and that is before it is encrypted.

#### Observations

**There is too much data** for any framework to effectively encrypt and decrypt as the speeds that would be required. Strong encryption would be impossible, and even hashing would be questionable.

**GPS positioning data is too slow** and inaccurate. IR and Ultrasonic sensors are too weak and prone to error. The only real substitute is video which means everything is being recorded from every angle all the time.

**Recording and analyzing video with Computer Vision in real-time would take a very powerful supercomputer**. Which shouldn’t be surprising because we are using organic supercomputers now ( our brains ).

**Protecting privacy would require that all PII ( like license plates and faces ) be obfuscated**. It’s unclear if obfuscating this much data in real-time is even possible.

#### Potential Attacks

**Opening cars to send and receive data makes the vehicles involved in V2V communication open to the possibility of injection and buffer overflow attacks**. An attacker could pivot from the V2V system to the other software or firmware in the car’s ecosystem. Privacy, of course, would be compromised especially if the encryption keys were stored in the car’s firmware, which most manufacturers do. If the keys were stored remotely the attacker would just simply comprise the channel on which the keys are distributed.

**Vehicles would have to identify themselves by reporting their position, therefore making it possible to know everything about someone's movements** ie [ Visited Midtown Safeway, Visited Midtown Cannabis Dispensary, Visited Therapy Clinic, etc ]. This information in the wrong hands could be weaponized. An attacker could exfiltrate the data before it was encrypted.

**With all cars sharing the same sensor data, an attacker could compromise the sensors to create a traffic jam** in order to cause confusion during a physical crime like a bank robbery.

**With cars sharing video data ( as described above ), and most cars connected to driver’s smartphones, an attacker could pivot from the V2V system to the car’s internal software, to the driver's phone using Bluetooth**, and transmit live video from inside the car using the target’s phone. The attacker could easily hide this elicit stream among the other video streaming to and from the car.

#### Conclusions

V2V sounds like a good idea, but it has a lot of implementation and logistical issues. Preventing collisions would be near impossible and would require sharing a vast quantity of unencrypted. Even then we don’t have AI fast enough or smart enough to make decisions to stop collisions. The best we have is an IR, Ultrasonic or Video sensor that might stop someone from hitting a wall or crossing a train track when a train is coming. But real-time decision making in traffic at 85MPH? I would trust a 16-year-old before I trust a machine.

Does V2-M-2V seem like a more viable solution? One where vehicles transmit minimal sensor information anonymously to a central server and vehicles could subscribe to a feed coming from the central server. Each broadcast would be read-only, so hacking it would be near impossible. This would not enable collision prevention but may augment the current GPS system. Using layered Sensor and GPS data the service could identify the driver’s relative position in a 500 SQft mesh of anonymous data. It wouldn’t require sharing anything, each driver just self identifies without sharing.

V2V seems cool, but I am not sure it serves any real utility unless we are watching iRobot. Will Smith makes everything look cool.