Short Range Vehicle Communication Security

Keith Galli, Gillian Belton, Juan Carlos Garcia
6.857 Computer Network Security
5/14/2019

Introduction

Overview

While connected cars are relatively new technology, they have made their way across the globe into the driveways and neighborhoods of millions of people. Connected cars, which allow a vehicle to have continuous access to the internet, have revolutionized the way we interact with our cars and the environment. Features such as contactless keys, entertainment and alarm systems, companion phone apps, Bluetooth applications and USB compatibility have all contributed to the slow decay of connected car security. As these flaws continuously surface, the world becomes more aware of the security challenges in front of us as we increase the capabilities and autonomy of vehicles.

On another side of the car industry, there is a lot of focus on driverless car technology. Car manufacturers pour computational power into machine vision and machine learning with the goal of vehicles being able to operate autonomously.

In this paper we focus on the intersection of these two areas. We envision a world where cars can not only operate autonomously using machine vision, but they can communicate detailed information with one another in real time through the utilization of their connected nature. There is a lot of significance to a future network such as this. For example imagine an ambulance rushing to get from point A to point B. With connected autonomous network, this ambulance could easily communicate to vehicles that it needs to get by which could lead them to automatically clear a path for the ambulance to get through. An additional example of the importance of a connected autonomous network can be seen with traffic. Traffic is often caused by a chain effect of asynchronous stopping. If vehicles could clearly communicate with one another when they are braking and when they are accelerating many traffic issues could be avoided.

In this paper we examine the current state of connected cars and their security. From here will build up to a future of connected cars where vehicle to vehicle messaging becomes more prevalent. We examine what types of security risks would arise in this type of network, as well as create simulation environment to visualize them. We conclude this paper by proposing a messaging protocol to secure vehicle to vehicle messaging.

Current State of Connected Car Security

As connected cars continue to increase in popularity around the world, engineers work to both secure connected cars and hack into them. The connected car's ability to send and receive messages at any time make it a target for network-based attacks. However, the history of connected car security involves more than just its ability to communicate between vehicles, but

also in its various IoT devices incorporated within. Bluetooth features, contact-less keys, and partner phone apps all open up connected cars to dangerous and concerning attacks. Over the past decades there have been dozens of documented successful hacks, and an equal amount of car companies rushing to patch up these vulnerabilities. In addition to the security vulnerabilities, we are interested in the current technologies being used to increase user safety and security. In the world of vehicle to vehicle communication, things are always evolving, but one protocol has stayed consistent: Basic Safety Messages, or BSMs. In this section we hope to explore the current state of connected car security, previous successful hacks, as well as introduce our element of focus: BSMs.

Threat Models and Known Vulnerabilities

The connected car's ability to have consistent access to the internet has opened it up to a wide variety of add-on Internet of Things (IoT) features. Services and separate electronics such as contact-less keys, vehicle partner phone applications, Car alarm systems, USB attachments, and Bluetooth accessories have all made their way into user's vehicles. These features incorporate a variety of hardware and software from different sources, which has only made it easier to hack connected vehicles in ways the car manufactures don't anticipate.

Partner phone applications are a classic example of a vulnerability in connected cars today. Many car manufacturers today include partner applications to go along with the user's new connected car. These apps allow users to remotely access the state of their car (unlocked or locked, location, milage, etc), sync music and contacts, or contact help in case of an emergency. While all these features are useful, if not properly protected they allow an adversary direct access to a vehicle's data and functionality. These applications often run on iOS, Windows, Android, or Linux, which allows hackers to exploit already established vulnerabilities in these operating systems, unrelated to the manufacturing of the car itself.

Contactless keys have also proven to be a difficult technology to secure properly. These remote keys work by emitting a signal over radio frequencies that can be used to unlock or start the engine. These signals can easily be detected, intercepted, or replayed, and the use of this technology has led to a dramatic increase in car theft. In the UK in 2017, the number of stolen vehicles rose to 89,000, an increase of 56 percent from the year before.

USB and Bluetooth technology have also both proven to be problematic as well. USB technology, which is usually a seperate piece of hardware bought by the car owner, presents a more hardware oriented vulnerability. USB devices such as music players, navigation systems, or charging components are often not thought as a security risk to your car. However, it is possible for an adversary to replace this hardware and inject a malicious script into the vehicle. Once this has occurred, an adversary can gain access to personal user data such as favorite locations, call history, passwords and text messages. Bluetooth is vulnerable as well, and when intercepted or exploited, can be used to steal the same set of user information.

Previous Attacks

There are many real world examples of the attack models described earlier. As more and more features are incorporated into connected cars, the more vulnerabilities that are discovered and exploited. One significant example of this was the BMW car thefts in mid 2017. The thieves were able to conduct a relay attack using multiple relay boxes placed carefully near both the vehicle itself, but also the owners home. By forwarding the radio signal of the key in the house, the thieves were able to artificially increase the range of the key's signal. Once it reached the car's OS system, the vehicle turned on and within seconds the thieves were gone. The entire process was completed in just over 60 seconds, a brutal awakening to those with contactless keys.

Another important instance of successful attacks against connected vehicles occurred in 2015. In this instance, two hackers were able to execute a remote attack on a Jeep Cherokee and take control of the vehicle. By sending malicious signals to the steering wheel and brake systems, the hackers were able to take partial control of the car. The break and steering electronic control units were still functioning however, and so the inherent safety mechanisms of the vehicle were not completely bypassed. Still, they were able to turn on the wipers, break at slow speeds and turn the wheel while in reverse. This attack was shocking to the world, and resulted in over one million vehicles being recalled. One year later, these same hackers successfully executed a much more powerful attack. Involving additional hardware this time, the hackers were able to send the break and steering electronic control units (ECU) into bootrom mode, essentially overriding the vehicles natural security measures. This allowed the malicious signals sent almost full control over the breaks, acceleration, and steering wheel.

These successful attacks are only a few of hundreds of documented vulnerabilities found in the last couple decades. They highlight some of the current issues of connected car systems, and were both eye opening to the world, bringing awareness to the work that still needs to be done to secure connected vehicles.

Basic Safety Messages

While many elements of connected cars have been evolving, coming, and going, the underlying communication protocols built into many vehicles have remained relatively constant and underutilized. At the forefront of this are Basic Safety Messages, or BSMs. BSMs were introduced by the department of transportation in the early 2000s to utilize the connected capabilities of cars and increase safety for all drivers. BSMs are messages transmitted approximately every 100ms, and contain information about the car's current state. This includes data such as, but not limited to, the car's latitude, longitude, heading angle, speed, brake status, steering angle, vehicle mass, and bumper height. The messages have a range of about 1 km, and are meant to be a low latency, localized broadcast. Notably, BSMs contain no unique identifier that belongs to only one specific vehicle. While not entirely anonymous, as vehicle

information is included, it is not used to keep track of individual drivers, but instead the environment itself.

BSMs have been used in the past to alert drivers of upcoming dangerous conditions, such as an accident, or an obstacle in the road, although they include a lot of data not being utilized fully. In the past BSM data has been used to evaluate the likelihood of an accident, based on long periods of monitored behavior of intersections or individual drivers. While these applications are interesting, we believe there are many more effective uses for BSMs in the future world of connected cars.

Future of Connected Cars

Potential of Communication based Driving

As autonomous vehicles become more prevalent in society, the design of transportation infrastructure and the communication protocols among vehicles will change. Roads in modern society were all designed with visual-based vehicle control systems in mind. Currently, a lot of information is conveyed with physical features placed throughout the road. Lines allow users to know where they can drive and when they can pass, stop signs and traffic lights allow vehicles to cross paths, etc.

In the future autonomous networks, peer to peer intercar communication will likely become a much more integral part of the autonomous network. In this new type of protocol, vehicles would send and receive messages among one another and take action based on the information communicated. This might not happen in the immediate future, but one can imagine that it is eventually a possibility. In a network such as this, vehicles could communicate with one another to dynamically change where lane boundaries are. This could help control traffic flow depending on the time of day. In addition, intersections could utilize short range communication to more efficiently let cars pass through than stop signs and traffic lights currently allow. BSMs have the ability to play a large role in enabling this type of behavior.

Threat Models and Potential Attacks

Security Goals

As communication between vehicles changes, new security measures will need to be put in place to accommodate. In this section we will examine the security goals of authenticity, availability, confidentiality, and integrity and how they relate to short range vehicle communication. This section will also detail examples of attacks that an adversary might make in this communication protocol.

Authenticity

Within our communication network, it is very important to be able to distinguish which messages are being sent by authentic vehicles. Because vehicles will take actions based on the messages they receive, a malicious party sending fake messages could have very dangerous results.

One such example is a Spam attack. In this scenario an adversary is able spoof fake messages for many different vehicles that do not actually exist in the network. The repercussions of an attack such as this is that valid vehicles would not know how to react to all of the noise and traffic might come to a complete halt.

Even if an adversary couldn't spoof messages for many different fake vehicles, there would still exist serious problems if they could spoof messages for a single fake vehicle. In a second type of attack, which we call the target collision attack, imagine a series of vehicles traveling in a straight line. An malicious party might read the position information from the lead vehicle and rebroadcast a fake vehicle message directly ahead of it. If this message is mistaken as a trusted one, the lead car might be forced to quickly apply its breaks which could lead to chain collision effect if trailing cars are unable to respond quickly enough.

Availability

A second goal of short range communication is for it to always be active. Basic Safety Message protocol includes about 10 messages being sent a second. It is important in our network for this to consistently happen. Vehicles should be set up with indicators that check to see if messages are being sent at the correct rate and that no content within the message has been corrupted.

One potential attack that compromises the availability of basic safety messages is a DDos attack. Even if a secure protocol was in place to only take action on authenticated messages, it is possible that an adversary generates hundreds of thousands of wavelengths in the Dedicated Short Range Communication (DSRC) spectrum. Even though vehicles would be able to identify these signals as invalid, they would have to use some amount of processing power to do this. If the amount of signals coming in exceeds the message buffer onboard vehicles, it is possible that some valid messages are dropped. This is a tough attack to defend against, but due to the limited range of DSRC signals (~1km) this type of attack would have to have coordinated efforts to create widespread effects. Regardless, vehicles should be able to resort back to visual based navigation if necessary.

Confidentiality

In car to car short range communication, confidentiality is not a security goal of high importance. This is because cars do not need to know any information about the driver or owner of the vehicle in order to successfully communicate. The only information relevant in

communication is the state of the cars involved. Thus a car identifier that is separate from the owner or person driver is suggested in car to car communication.

Integrity

The integrity of the data transmitted in a Basic Safety Message is of complete importance. This means no car participating in the communication network should be able to send out false data (such as incorrect speeds, size, position, etc). As pointed out in *Threat Models and Known Vulnerabilities*, connected cars have been hacked and can be hacked. Thus in creating a secure message protocol, we assume that the software and hardware running the BSM algorithms onboard a car are secure. In summation, the BSM software onboard a participating car and the messages sent cannot be tampered .

If data can be tampered with, it makes no sense to trust the messages sent. Any valid car in the network could then send out false information and wreak havoc on the roads. A possible attack would be for an adversary, note who has purchased a valid car that communicates in our network, to send false positions into the network. Any listening car would have to respond to these fake positions as if they were real. In our simulation environment, we created an attack in which an adversary sends false positions into the network and cars are forced to stop, allowing the adversary to have the road completely for themselves.

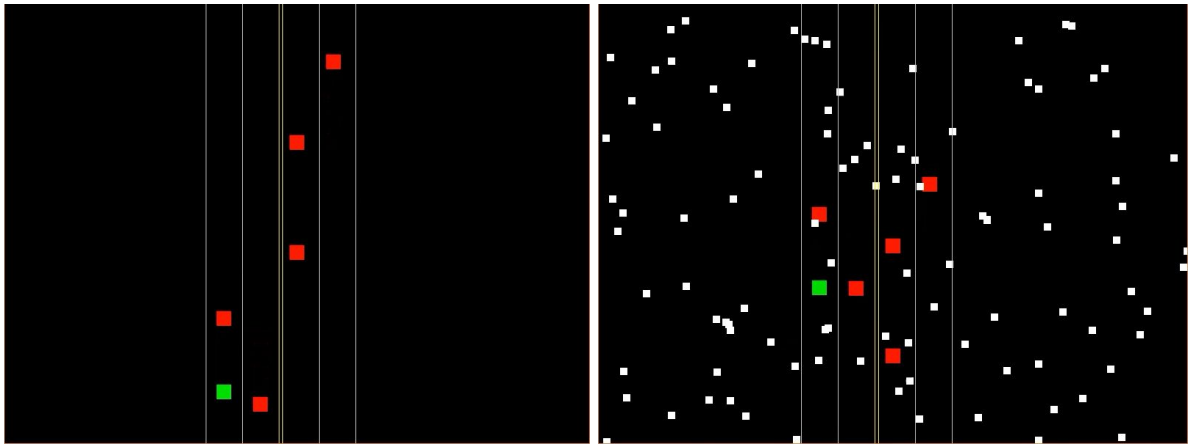
Simulation Environment

One component of this project was creating a simulation environment to test out short-range BSM communication protocols. This was implemented in Python and is publically available on GitHub (https://github.mit.edu/jcgarcia/ConnectedCarSecurity). A main goal of this environment was to be able visually explore communication details and potential security threats.

A simulation consists of any number of valid vehicle objects each with their own movement properties along with a set of defined streets and intersections. Each one of these vehicles broadcasts its BSM message to all other vehicles in the environment. The vehicles respond to incoming messages by slowing down if a collision might occur or continuing on their path otherwise. User defined malicious vehicles can also be added to a simulation. Malicious vehicles override the broadcast message function and instead of sending actual movement information, they can spoof any number of fake messages in locations of their choosing.

In one experiment we performed, we created a demonstration of the spam attack described in the Authenticity section above. In this simulation, valid cars (represented as red and green blocks) were moving up and down a set of parallel streets. When no malicious party is present, they move steadily to their destination (left image). When a malicious party is

introduced who spams the network with randomly generated fake BSMs (small white blocks), all valid vehicles are forced to stop (right image). Pictures of this simulation can be found below.



Security Solutions

Digital Signature Scheme

In order to secure BSM communication between authentic vehicles in the network, we propose a hierarchical trust system and the Signed Basic Safety Message (SBSM) protocol. The figure below captures the hierarchy we use in SBSM protocol.

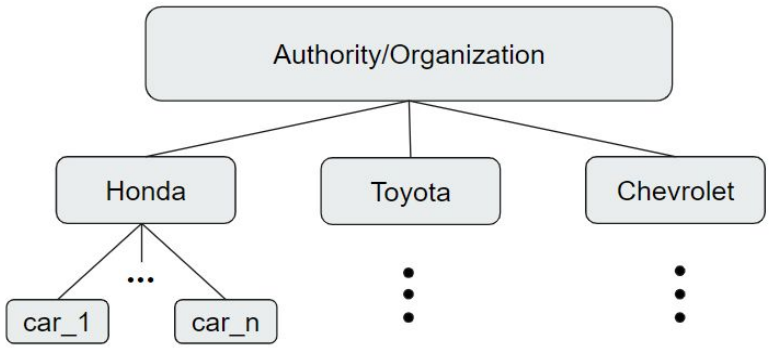


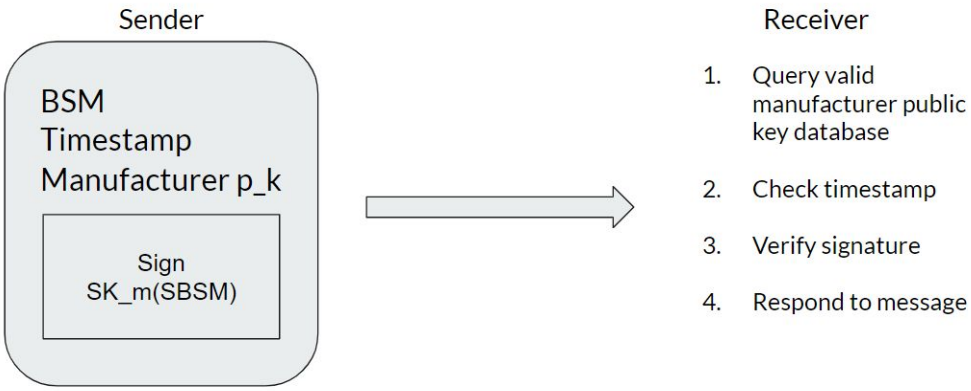
Figure: The hierarchy used for the "chain of trust" in the SBSM protocol.

At the top of the hierarchy is a central authority or organization that chooses which manufacturers have permission to produce vehicles that will participate in the SBSM protocol. Each authorized manufacturer has its own public and private key, p_{m_i} and sk_{m_i}. A manufacturer authorizes the cars it produces by embedding its private key into the vehicle's hardware. This private key is used to sign each BSM a vehicle produces. Furthermore, each car participating in the SBSM protocol will locally store the public keys of all valid manufacturers and the central

authority. Consequently when transmitting messages, a car can use the stored public keys to verify the validity of a car in question. Note that the central authority also has the role of keeping an up to date list of the trusted manufacturers in the network. If a specific private key is ever compromised, the central authority can remove the manufacturer from the trusted list until the problem is solved.

The specific details of the message protocol is as follows. Each vehicle in the network acts as both a sender and receiver of SBSMs. On the sender side, a vehicle will create a message which contains in plain text the basic safety message content, a timestamp, and the vehicle's manufacturer's public key p_{m_i}. The sender will then digitally sign the content using the manufacturer embedded private key sk_{m_i}. This digital signature will be concatenated onto the original message and then broadcasted out to the network.

On the receiver side of the protocol, upon getting a message the first check will be to see which manufacturer it came from. This is done using the public key attached to the SBSM. Next the receiver should query its internal database to confirm that this public key is trusted by the central authority. This internal database can be periodically updated by the receiver to make sure the set of current trusted parties is correct. Next the receiver should confirm the timestamp is within a few seconds of the current time. This is to ensure that an adversary isn't performing a replay attack with a message that was valid at an earlier time. If this check passes, the receiver can then verify the digital signature of the message it received using mentioned public key. If the signature is verified, the vehicle should take action that corresponds with the content of the BSM. A diagram of this process is below.



Secure Hardware

One of the assumptions of the digital signature scheme mentioned in the last section was the ability to securely embed private keys in vehicles. While this is still a developing area, there has been active progress in similar technology. One such example is Apple's Secure Enclave which is built into some of the newest iOS devices and MacBook Pros. The Secure Enclave is a hardware-based key manager separated out from the main processor. The Secure

Enclave creates and stores private keys and is also able to perform operations using them such as digital signatures. A major detail of this is that the private key can never be physically accessed by the main processor. All the main processor can access is the results produced by the cryptographic operations. If applied to vehicle communications, this could mean that a vehicle could sign basic safety messages without an adversary who has access to the main vehicle's processor being able to listen in and steal private key information.

Conclusion

While the majority of cars on the road are yet to be connected to the internet, we can only expect the number of active connected cars to increase as time progresses. The security of car communication, whether it be through the internet or smaller vehicle-to-vehicle networks, is of utmost importance in a connected car future. If security is compromised, connected cars can be taken control of or misguided by adversaries. In doing so, an adversary could control traffic and force collisions. At the root of car communication is the Basic Safety Message. Through this project we introduce a Secure Basic Safety Message protocol.

In designing the SBSM protocol the most important security measures were authenticity and integrity. In car communication it is incredibly important that message content not be tampered with and that the message is coming from a valid vehicle. The SBSM leverages a chain of trust to establish which vehicles are valid. Cars are embedded with a manufacturer's key and use public key cryptography to verify the validity of an incoming message.

In order to explore the SBSM protocol we programmed a simulation environment with roads, intersections, cars, and malicious cars. In the environment we simulated attacks and defenses that convey the importance of secure communication and the effectiveness of the SBSM protocol. One can imagine a future in which cars are operating fully by means of communication. And, in this future, a protocol like SBSM will be necessary.

References

Paper links:

https://www.researchgate.net/publication/305842438_Improved_warning_and_assistance_information_from_connected_vehicle_basic_safety_messages

https://journals.sagepub.com/doi/10.1177/0361198118773869

https://developer.apple.com/documentation/security/certificate_key_and_trust_services/keys/storing_keys_in_the_secure_enclave

https://www.cambridge-news.co.uk/news/uk-world-news/prevent-keyless-car-stolen-theft-14712880

BMW Stolen

https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/