Automotive Security – Where should you focus?

Not all Security Threats Are Equal

Chuck Link, President and CTO, M2MD Technologies, Inc.

As the automotive industry has added connectivity and remote control features, the vehicle has become more vulnerable to hacks. Most major manufacturers have been in the news for a security breach of some form or another. The FBI along with the Department of Transportation and NHTSA issued a public service announcement in March 2016 stating that "with this increased connectivity, it is important that consumers and manufacturers maintain awareness of potential cyber security threats." With so many potential threats and so many different ways to address the problem – where should you focus?

First, think of all of the entry points a bad actor could use to access the vehicle – in other words, the potential attack surfaces. Most vehicles today support connectivity, data input and remote control of various features, including the cellular connection, Bluetooth, Wi-Fi access points, RF-enabled key fobs, the on board diagnostics (OBD) port, the tire pressure monitoring system and various CD/DVD, USB, and audio input methods to name a few. Each of these attack surfaces presents an opportunity for a threat to penetrate and issue a command to an internal computer-like controller known as an Electronic Control Unit or ECU. ECUs control starting, braking, throttle (accelerator or gas pedal), door access, airbags and dozens of other safety and vehicle control units, including steering in some cars. Unauthorized messages or commands to these ECUs result in the hacks that make front page stories.

Once the attack surfaces have been identified, remediation should start with the threat that presents the greatest risk. An argument can be made to focus on the attack surfaces that have the greatest potential to impact the safe operation of the vehicle. However, access to any of the attack surfaces referenced above could have an impact on vehicle operations. Risk exposure should consider the total number of vehicles that may be accessible by a single perpetrator in the shortest timeframe. Accordingly, the number one risk is a vulnerability that can be exploited remotely and allow a single bad actor to impact multiple vehicles without the risk of physical detection.

Most attack surfaces referenced above require access to the vehicle or at least close proximity in order to penetrate. For example, attacking through the USB ports, audio inputs, or OBD port will require direct access to the vehicle. Attacking wirelessly through the key fob, Bluetooth or Wi-Fi access feature requires local presence. But, the cellular connection found in an embedded telematics control unit (TCU) of a vehicle or an aftermarket OBD based telematics solution that includes a cellular module could theoretically provide access from anywhere in the world. According to well-known security researchers Charlie Miller and Chis Valasek, this cellular connection is the holy grail of automotive attacks since the range is quite broad (i.e. as long as the car can have cellular communications). Additionally, most telematics programs offer a growing list of features that can unlock, start, locate, and even disable a vehicle or

update firmware in vehicle ECUs. A combination of the extensive functionality and access from anywhere puts this attack surface as the most important attack surface to protect. Since automobile security is tightly related to safety, a security breach could result in perpetrators placing occupants in danger.

To secure the cellular channel, many automakers are using certificate based operations that utilize the public key infrastructure. Certificate based security was designed for the public internet where the two devices – think your computer and your bank's server – are unknown to each other. The authentication process using certificates requires a computationally intensive handshake that takes time and requires the devices to pass data back and forth to establish a secure session. When using a computer on a home or office network, this transaction happens quickly (due to the processing power of your computer) over a data circuit with a nearly unlimited data budget and a high bandwidth. To minimize the cost and battery consumption, TCUs typically have far less powerful processors adding to the time required to complete the certificate exchange. In addition, wireless operators charge automakers by the amount of data transmitted over the network making the data consumed in the handshake process relatively expensive compared to other types of data usage.

There are other challenges using certificates in automotive applications. Certificate operations were designed for human intervention. They have expiration dates and therefore require updating from time to time, and in the event of an error, there is no screen or keyboard allowing for human interaction to resolve. If a certificate is compromised, a trip to the dealer could be the only way to resolve. After all, if a certificate is compromised, how do you trust the replacement? In addition, certificates are also vulnerable to common attacks such as "man in the middle" and "internet sniffers", and with Quantum computing looming in the next decade, these high speed computers may be able to mathematically compromise a certificate with ease in vehicles rolling off the production line today. In addition, with certificates, a single key-pair is used to secure all encrypted communications, so a breach of a single private key can potentially compromise every vehicle's communications.

While certificate operations are an acceptable form of security for broader Internet applications, it is not the optimal answer for the automotive industry. In automotive telematics, the cellular communications happen on a private network and between two known devices that have been preconfigured to work together making the certificate exchange and handshake costly and unnecessary. Automakers should still use a proven, tested security solution – Transport Layer Security (TLS) 1.2 – but in a manner that is fast, cost effective and designed for the unique automotive environment.

M2MD Technologies has developed a patent pending solution that combines TLS 1.2 with the security of the wireless SIM card to generate an extremely secure solution without the uncertainty and logistical challenges of certificate based solutions. TLS with M2MD's SIM solution provides an efficient method for securing communications with the vehicle that decreases both the communications costs and the number of servers required to support the connectivity by a factor of 20 and reduces the time required to establish a secure session.

M2MD's solution allows for the periodic updating of the vehicle's security credentials – both in the case of compromise or just for good security hygiene. This method along with the other features in the M2MD communications gateway provide automotive manufacturers with a faster, less expensive to operate and far more secure method for cellular connectivity to the vehicle.

# # #

About the Author

Mr. Link is the President and Chief Technology Officer for M2MD Technologies, Inc., a company focused on securely connecting machines to mobile devices. Previously, Mr. Link was Chief Technology Officer and a co-founder of Hughes Telematics, Inc. (now known as Verizon Telematics Inc.), where he served as the Chief Technology Officer from the company's inception through its acquisition by Verizon in 2012 until he departed in early 2015. Mr. Link was responsible for the technology foundation of the company and focused on vehicle connectivity, network architecture and strategy for the company's OEM telematics offerings. Most recently, Mr. Link led the successful technology rollout of services for Mercedes and Volkswagen in China.

www.m2mdtech.com
Twitter: @M2MDTECH
LinkedIn: M2MD Technologies, Inc.
Media Contact: PR@m2mdtech.com