Next Generation Automotive Cybersecurity with Software Defined Perimeter & Blockchain

Mahbubul Alam
CTO and CMO
Movimento Group

Alam has been reinventing technology and strategy at Movimento since 2015. Prior to this, he spent 14 years as a technologist at Cisco were he was leading its IoT and M2M platforms since 2012.

The emergence of autonomous vehicles is radically changing the automotive business. This change is bringing in new revenue generation opportunities for the whole industry, but with it, also new risks - specifically cybersecurity. Since autonomous vehicles are completely dependent on connected software for all aspects of their operation, they are vulnerable to a broad spectrum of cybersecurity attacks. As we see in the news every day, even well-established sectors like the financial industry and government agencies are still struggling to deal with the same issues. Subsequently, the automotive industry will actually have to leapfrog existing approaches to cybersecurity to ensure that all existing threats are mitigated but also that future "unknown" threats are prevented. Automotive cybersecurity is much more than ransom, data breach, stolen personal records, etc. - it is about the safety of our lives!

The recent sanction of an automotive-specific cybersecurity bill in the US congress, H.R. 3388, also known as the "Self Drive Act", and the Senate's advancements on the AV START Act have sent a clear signal that the automotive industry needs to get serious about cybersecurity. The immediate security risks to connected cars and long-term risks to autonomous vehicles must be addressed. The "Self Drive Act" outlines the cybersecurity plan for autonomous driving systems.

Traditionally, the automotive industry only adopts mature technology. Unfortunately, the rapid pace of software development requires the automotive industry to become more innovative with respect to how it views software. More importantly, the dramatic increase in cybersecurity attacks demands cooperation among OEMs, Tier-1 suppliers, software developers and cybersecurity firms at a scale that has never been reached before. Today's automotive cybersecurity solutions in the marketplace are at best an after-thought. There are still many unanswered questions including how to safeguard internal vehicle systems from attacks, ensure data integrity while also providing data privacy and secure vehicle-to-cloud communications in millions of vehicles that each supports hundreds of ECUs, sensors, domain controllers, radars, LiDAR and ADAS. In order to deliver cybersecurity solutions to address these specific questions for connected and autonomous vehicles, a number of factors must be considered such as scaling globally to a massive number of vehicles, detecting software tampering and malware, support an array of telematics, information and safety applications, enabling precision access control to vehicle software suppliers and meeting regional safety, privacy and driving regulations.

Fortunately, there are two new emerging technologies, Software Defined Perimeter (SDP) and Blockchain, that offer a path forward. SDP enables the provisioning of secure communications between the software process within the vehicle and cloud-hosted applications while Blockchain enables secure messaging. By combining the any-to-any connectivity of the SDP with the scale of the Blockchain, an efficient cyber security model for connected and autonomous vehicles can be created. In order to further provide secure connected and autonomous vehicles in a systematic manner and provide the required safety, a number of practices should be adopted:

- Incorporate an industrywide Automotive Cybersecurity Lifetime (from cradle to grave) Compliance Certification program. Make cybersecurity a mandatory part of a vehicle's product development process.
- Establish a joint automotive cybersecurity taskforce that is responsible for proactive prevention, mitigation and correction of threats and attacks.
- Provide regulatory agency access to vehicle metadata (non personally identifiable information) for random cybersecurity compliance checks and validation.

What is a Software Defined Perimeter (SDP)?

SDP is a new approach to cybersecurity that is designed to provide on-demand, dynamically provisioned secure network segmentation, that mitigates network-based attacks, by creating perimeter networks anywhere in the world, whether it is in a cloud or in a data center. The architecture comprises of three main components:

- Virtual Gateway: A SDP virtual gateway is deployed in a cloud, data center or a connected gateway in the vehicle depending on the use case. This SDP virtual gateway combines the functions of a Firewall, VPN and application layer gateway in a single virtual appliance by only allowing approved software on authorized devices to connect to protected applications inside the vehicle as well as to the cloud.
- Client: To allow vehicle software processes to connect to protected applications, they must utilize the SDP client which can be embedded inside e.g. an over-the-air (OTA)

software management and data client. This SDP/OTA client has three distinct purposes. Firstly, it allows the automotive policy engine to determine the vehicle identity. Secondly, it allows the remote analysis of software and system processes to detect the presence of malware. And lastly, it provides a secure application layer connection between a software process or ECU inside the vehicle to a software process on a cloud application server.

- Controller: Tying the SDP/OTA client and gateway together is a controller. The SDP controller functions as a hub between the client and the gateway as well as external policy systems.

The SDP's interlocked security controls protect software systems within a vehicle and their data from cybersecurity attacks. All SDP transactions are cryptographically certified to mitigate real time tampering while the architecture scales to millions of vehicles supporting billions of software modules and ECUs.

What is Blockchain?

Blockchain, also known as Distributed Ledger Technology (DLT), is a decentralized database for ledgers and transactions. Bitcoin, also known as cryptocurrency, is one of the most famous and widely adopted global virtual currencies in the world and is based on Blockchain. Users gain access to their Bitcoin balance using their private key.

Being immune to a single point of failure and security issues provides a lot of advantages to Blockchain compared to traditional databases. The main advantages of the Blockchain are its immutability, scalability with data security, high data integrity, super transparency (all nodes have visibility into every messaging/transaction metadata) and its ultra-low cost per message/transaction making it very suitable to e.g. micro-payments. Deployments of Blockchain can be either public or private, where, in a public Blockchain (permission-less), any node on the Internet can read from and write to the ledger with appropriate application whereas, in a private Blockchain, all the nodes in the network are known and have explicit permission to read and write the ledger.

The above-mentioned Blockchain characteristics make it ideal for automotive use cases and OEMs could use a private Blockchain as a platform to enhance their overall cybersecurity for vehicles, validate software bills of materials, enable cost effective micro-payment, strengthen identity management and improve data validation. Examples include pooling of data from vehicles, fleet management, optimize business processes, enable peer-to-peer mobility sharing capabilities that can all disrupt existing business models and improve overall operations.

Combining Software Defined Perimeter and Blockchain for Automotive

Blockchain enable secure messages that can carry a wide variety of payloads from the status of sensors to the delivery of private encryption keys while an SDP provides secure in-vehicle and Internet links. Thus, blockchain messages can be used by ECUs to signal management systems on their status. If a situation requires a secure bi-directional link, an SDP connection can be provisioned from a vehicle-to-cloud resource and, once set up, Blockchain can be used to transmit messages between internal vehicle systems. The combination of SDP and Blockchain technology creates a system that is very lightweight and scalable, and yet has the ability to create secure enclaves when required. In addition to supporting telematics and safety applications, this Blockchain/SDP platform can also support multiple cryptocurrencies such as Bitcoin or Ethereum and thereby be a critical digital payment foundation for the automotive ecosystem.

A simple, but powerful example, of how short Blockchain messages and SDP connections complement each other, is the challenge of driving an autonomous vehicle in the snow. As an autonomous vehicle drives through a snowstorm, it can continuously send Blockchain status messages to cloud-based safety monitoring systems. However, if the vehicle gets stuck in the snow and is unable to dislodge itself, a secure SDP connection can be provisioned which will backhaul all the vehicle image sensors to a specialized cloud application for processing.

Key Takeaways

Both SDP and Blockchain represent the cutting edge of technology. For example, Gartner listed SDP as one of the most important new technologies in 2017 to reshape the enterprise market. Similarly, Blockchain is being adopted as a secure messaging protocol in a wide variety of applications due to its low cost and high scalability. The automotive industry could adopt both technologies as a foundation for secure OTA software/firmware/content updates, secure data exchange and autonomous driving communications. Both Blockchain and SDP are open license free public domain standards and both concepts are proven in large-scale critical deployments in areas such finance and tele communication. This restriction-free model means that there is no barrier for the automotive industry to adopt and innovative on top of them.

With attacks rising every year, cybersecurity has become one of the most important focal points for the automotive industry. A disruptive approach must be incorporated to battle the threat of cybersecurity attacks that are becoming more sophisticated each day. With the Blockchain-based SDP, OEMs have a unique solution that can empower the global automotive industry to secure connected cars and autonomous cars with confidence. ▪▪■

Junaid Islam
CTO
Vidder

Junaid Islam is the CTO and founder of Vidder, which provides distributed access control solutions to Fortune 500 companies. Prior to Vidder, Junaid founded Bivio Networks, which developed the first Gigabit speed software-based security platform in the industry. Earlier in his career, Junaid helped create networking standards such as Frame Relay, ATM and MPLS at StrataCom and Cisco.