**First Milestone Report**

**David Kelly**

**7/3/2021**

**Title**  
Improve the process of updating software in electric vehicles by making sure that the update has been approved using customer credentials.

**Description**

The contribution is to recommend that the updates of software would require that the customers credentials be validated using multi-factor authentication. Biometrics, tokens, userId/password and sms should all be considered.

**Status of the Project**

I have been reading these documents and others to gain an understanding of the OTA update process.

Scooter Dolls, “Over-the-air updates: How does each EV automaker compare?”, April 2021, <https://electrek.co/2021/04/01/over-the-air-updates-how-does-each-ev-automaker-compare/>.

I. D. Foster, A. Prudhomme, K. Koscher, and S. Savage, “Fast and vulnerable: A story of telematic failures,” in Proc. of USENIX workshop on Offensive Technologies, 2015, pp. 1–9.

**Status of the Milestones:**

1. Milestone 1 is complete: Find out what vehicles need software updates.

The following vehicles need updates:

Audi, BMW, BYD, Canoo, Faraday Future, Fiat Chrysler (FCA), Ford, General Motors (GM), Honda, Hyundai Motor Group (Hyundai/Kia/Genesis), Jaguar/Land Rover, Li Auto, Lucid Motors, Mercedes-Benz, NIO, Nissan, Polestar, Porsche, Rivian, Tesla, Toyota, Volkswagen (VW), Volvo, Weltmeister (WM Motor) and Xpeng.

1. Milestone 2 is complete: For each vehicle, document the software update process.

Each vehicle requires different systems to be updated such as infotainment centers, brakes, self-driving systems, motors, security systems, etc.

I did not find any multi-factor authentication being used to authenticate the updates. For instance, Tesla cars receive OTA updates regularly. The customer can update immediately without any more verification.

1. Milestone 3 is complete: Find security threat potential in each vehicle update process.

OTA updates would be vulnerable to several of the STRIDE attack vectors. Spoofing can be used by not being authenticated to update certain components. Tampering is possible with which components are being updated. Elevation of privilege is also a concern if a customer is not authorized to update the components.

**Milestones yet to be accomplished**

Milestone 4: Recommend security changes for each vehicle update using MFA.

Milestone 5: Propose how the customers credentials will be applied for any software update.

**Proposed time line to accomplish the remaining milestones**

Milestones 4 and 5 will be accomplished at the second milestone report.