**Project Proposal**

**David Kelly**

**Title**

Customer credentials should be used when updating vehicle software.

**Motivation and Problem**

The process to update software in vehicles has been left to mechanics and dealers without consistent customer validation and use of secure credentials. We should treat software in our vehicles the same way we do for cell phones, laptop or desktop computers. Updates such as Over the Air (OTA) should make sure that the user credentials are first checked. Without strong security, the updates could be compromised using threats of tampering or spoofing. Also, the customer may want to reject certain updates. Updates that happen at the repair shop should use customer credentials before updates begin. An attacker could try to update your software while you are driving and cause an accident and harm the passengers. If the credentials are needed for each update, this type of attack would be harder to accomplish.

**Description of the Contribution**

The contribution is to recommend that the updates of software would require that the customers credentials be validated using Multifactor Authentication (MFA). Biometrics, tokens, UserID/Password and SMS should all be considered. The scope of this paper applies to newer vehicles containing a software update interface.

**Proposed Milestones**

1. Find out which vehicles and items have software installed that need software updates. Updates might include the engine, brakes, music, GPS, cameras, infotainment center, etc.
2. For each vehicle, document the current software update process.
3. Find security threat potential in each vehicle update process.
4. Recommend security changes for each vehicle update using MFA.
5. Propose how the customers credentials will be applied for each software update.

**Proposed time line to accomplish the milestones**

1. Milestones 1-2 will be completed at the first milestone report.
2. Milestones 3-5 will be completed at the second milestone report.