Client/Company/Organization: ISU Digital Ag

Submitter Name: John Potter   **Email:** jrpotter@iastate.edu

Project Contact: **Email:**

Project Title:

Mobile Vehicle Cybersecurity with On-board Key Management

Project Abstract:

Vehicle CAN Bus networks for heavy-duty trucks, buses and off-road machinery are currently standardized through SAE J1939 which is an open, non-secured network. As Original Equipment Manufacturers (OEM) change their business models to be option/subscription based – raising the value of information on the vehicle network, and as more aftermarket manufacturers provide systems that require plugging untrusted devices into vehicle networks (for data gathering, system monitoring, and other value-add activities) it is in the interest of all parties (owner/operators, OEMs, and aftermarket manufacturers) that the data flowing through the vehicle network is authentic and has not been intentionally or unintentionally modified (i.e., messages have integrity), particularly as it relates to command-and-control messages.

This project will implement protocols used for on-board key management and secure message exchange defined in SAE J1939-91C (a draft specification for securing in-vehicle communications using CAN Flexible Data (FD) network technology).

This project simplifies one important aspect of vehicle network security: it assumes a free-form approach to CAN FD frames, as opposed to being constrained to J1939-22.

The project team will be responsible for designing and implementing the vehicle security interfaces and will achieve a full hardware demonstration.

Expected Deliverables:

1.   Demonstrate technical ability to work with CAN FD segments.
2.   Demonstrate implementation of key management protocols specified in J1939-91C (which allows for on-vehicle generation and sharing of session keys without requiring OEMs to inject secrets)
3.   Demonstrate use of generated key to secure messages using CAN FD frames.

Specialized Resources Provided by Client:

Client will provide technical student mentoring and guidance throughout the project. No other unique or highly specialized infrastructure or resources are required.

Anticipated Cost: **Financial Resources Provided by Client:** All costs of hardware or supplies required for this project will be provided by the sponsor.

Preferred Students for the Project:

- ☑ Electrical Engineering
- ☑ Computer Engineering
- ☑ Software Engineering
- ☑ Cyber Security Engineering
- ☐ Other:

Other Special Skills:

Anticipated Client Interaction (estimate):

- ☑ 1 meeting per week
  - ☑ In person, ☐ Over the phone, ☐ Web / video conferencing
- ☐ 1 meeting per month
  - ☐ In person, ☐ Over the phone, ☐ Web / video conferencing
- ☐ 2 or more meetings per month
  - ☐ In person, ☐ Over the phone, ☐ Web / video conferencing
- ☐ 1 meeting per semester
  - ☐ In person, ☐ Over the phone, ☐ Web / video conferencing

Meeting ABET Criteria

Please rate the following statements as they relate to your proposed project:

0 – Not at all	1 – A Little	2 – Somewhat	3 – A Lot	4 – Completely

Statement	0	1	2	3	4
On this project, students will need to apply knowledge of mathematics, science, and engineering	☐ 0	☐ 1	☐ 2	☐ 3	☑ 4
This project gives students an opportunity to design a system, component, or process to meet desired needs within realistic constraints such as economic, environmental, social, political, ethical, health and safety, manufacturability, and sustainability	☐ 0	☐ 1	☐ 2	☐ 3	☑ 4
This project involves students from a variety of programs, i.e., CprE, EE, and SE	☐ 0	☐ 1	☐ 2	☐ 3	☑ 4
This project requires students to identify, formulate, and solve engineering problems	☐ 0	☐ 1	☐ 2	☐ 3	☑ 4
This project gives students an opportunity to use the techniques, skills, and modern engineering tools necessary for engineering practice	☐ 0	☐ 1	☐ 2	☐ 3	☑ 4

Project Approval – *for use by ECpE Senior Design Committee*

- ☑ Approved: sdmay23-proj015
- ☐ Project Assigned:

☐ Advisor(s) Assigned: _____

_____

_____