Toward a Test Bed for Heavy Vehicle Cyber Security Experimentation

Rose Gamble, Jeremy Daily , University of Tulsa (#1619690)
Indrakshi Ray, Colorado State University (#1619641)

Can a bus or truck be hacked? If so, can a whole fleet be hacked?
What role does the smart highway play in truck or fleet vulnerability?
What test beds are needed to allow experiments to assess vulnerability?

- **Challenges**
  - Cyber assurance of heavy trucks is a major concern with new designs as well as with supporting legacy systems
  - Many cyber security experts and analysts are used to working with traditional IT networks and are familiar with a set of technologies that may not be directly useful in the commercial vehicle sector
- **Research Objectives**
  - Prototype a remotely accessible testbed using actual hardware, sensor simulation, CAN, and J1939
  - Exploit the openness of the CAN network and the J1939 protocol specifications
  - Experiment with attack vectors, such as the potentially vulnerabilities related to telematics units
  - Investigate the capability needs of an intrusion detection system

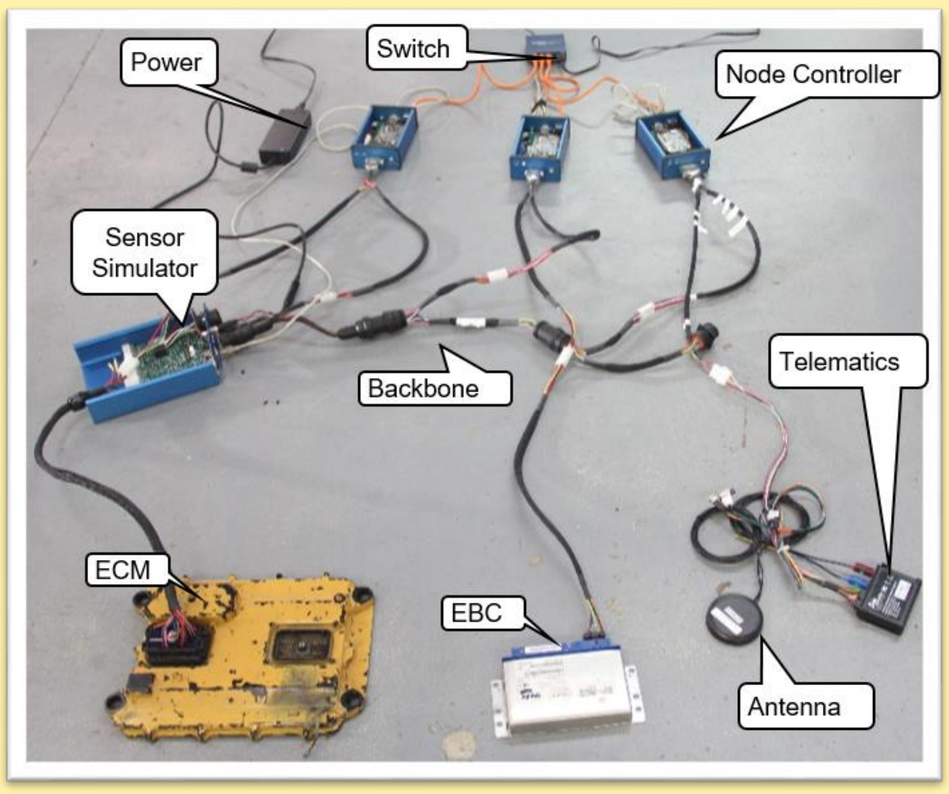

Fig. 1: Layout of a remotely accessible test bed

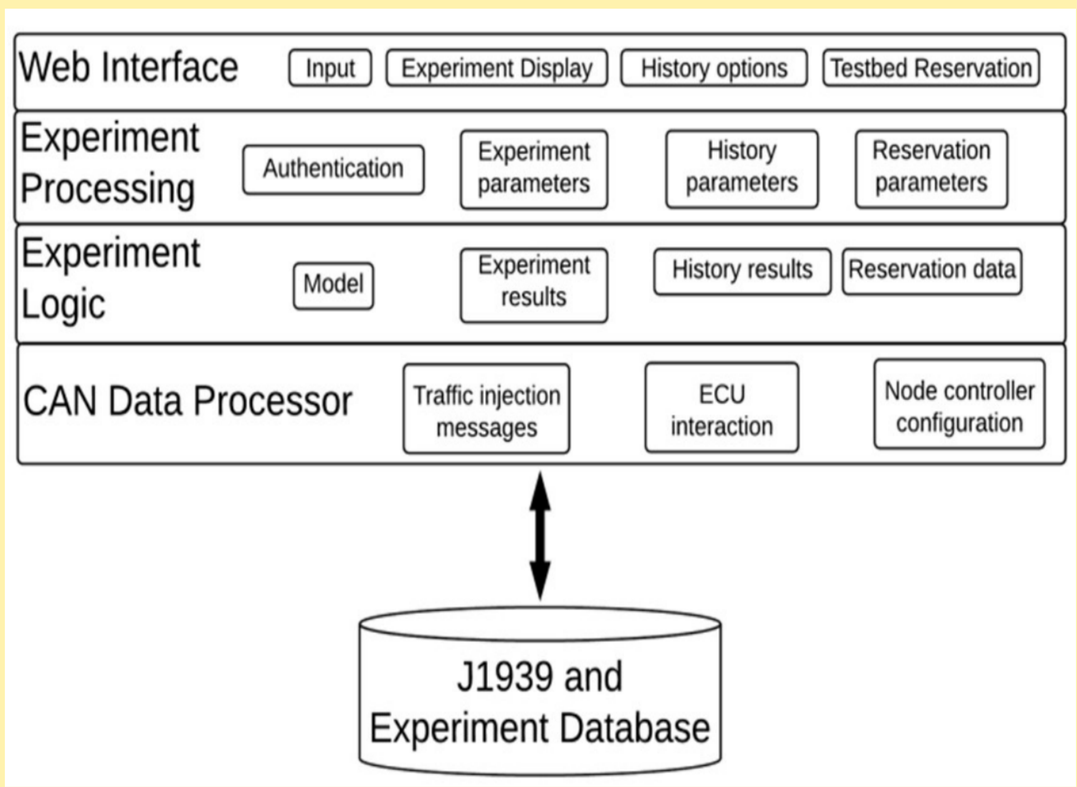

Fig. 2: Software Architecture of the Remote Interface to the Testbed

Approach

- Construct the physical test bed with an engine control module (ECM), an electronic brake controller (EBC), and a telematics unit through sensor simulator to a CAN network using the J1939 protocol.
- Create the remote interface to the test bed to additional experimentation
- Use the test bed to simulate the functions the ECUs to control attack experiments.
- Establish if the J1939 protocol is exploitable by perform attacks that are similar to those which have been executed on the OSI layer protocols.
- Investigate Bluetooth data transmission vulnerabilities and determine if the same attack vectors exist with telematics units.
- Open the test bed to external researchers for investigation

Current results

- Test bed and remote interface prototyped
- Can sniff Bluetooth traffic, follow a connection from the telematics unit to a driver's cell phone, and decode the packets
- Demonstrated 3 specific denial-of-service attacks using the J1939 data-link layer request and connection management protocols.

Ongoing work

- Build out the test bed with additional electronic control units
- Fully implement the remote interface
- Identify attacks that can act as a motivation to extend the current logic for in-vehicular IDS
- Use any vulnerabilities found to create additional mitigation strategies and uncover new directions to vehicular security research.

Interested in meeting the PIs? Attach post-it note below!

The 3rd NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
January 9-11, 2017
Arlington, Virginia