Summary of Reading List

By Jia Zhou

Part 1:

http://web.eecs.umich.edu/~ktcho/

Researcher: KYONG-TAK CHO (조경탁) from University of Michigan

Publication :

- (CCF A 类)CCS'17, Viden: Attacker Identification on In-Vehicle Networks
- (CCF A 类)CCS'16, Error Handling of In-vehicle Networks Makes Them Vulnerable
- (CCF A 类)SEC'16, Fingerprinting Electronic Control Units for Vehicle Intrusion Detection
- ICCPS'15, CPS Approach to Checking Norm Operation of a Brake-by-Wire System

These papers can be divided into two parts, defense and attack.

Defense :

To build an Intrusion Detection System to detect anomaly, vehicle misbehavior, and cyber-attack within in-vehicle network automatically.

1. Checking consistency between the driver's intention and data (braking behavior and environment).
   ICCPS' 15
2. Exploiting the message periodicity for clock skew estimation, which are then used to fingerprint the transmitter ECUs.
   Sec' 16
3. Exploiting small inherent discrepancies of CAN output voltages when sending a 0-bit between different ECUs, to fingerprint ECUs and can be used for attacker identification.
   CCS' 17

Attack (find new vulnerabilities):

1. Exploiting error-handling scheme of in-vehicle networks to disconnect or shutdown good/uncompromised ECUs. It's one type of DoS(Denial-of-Service) attack.
   CCS' 16

Part 2:

Details as below:

ICCPS' 15:

Objective:

To detect unpredictable misbehavior for the Brake-by-Wire system based on an anomaly detection method.

Method:

1. Build a tire-friction model(摩擦模型) as a norm model for anomaly detection. Choose the Brush model from [1].
2. Check the norm operation of braking.

By checking consistency between the driver's intention, braking behavior and environment to detect misbehavior of vehicle. If any vehicle behavior is inconsistent with the driver's intention of the environment, such as the driver presses the brake pedal intending to slow down the vehicle, but the vehicle is accelerating actually, this paper construct a real-time consistency check system to detect such misbehaviors.

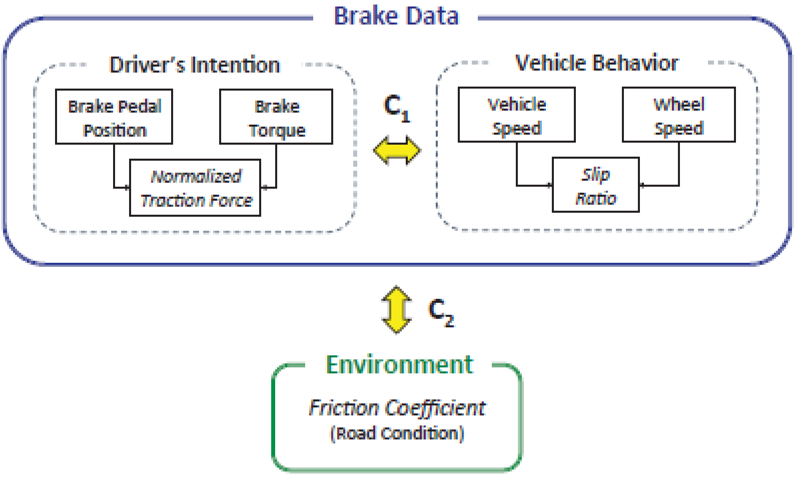


Figure 2: Checking consistency between the driver's intention and vehicle braking behavior, and brake data and environment.

Experiment:

Simulation, not on a real vehicle: Use CarSim to obtain realistic sensor readings for the slip ratio and the normalized traction force.

My conclusion:

- It's not exactly a security problem, it detects misbehaviors of vehicle, not attack. There is no discussion about attack model in this paper. But it can help improve automotive security and safety.
- It's an intuitive thinking to detect misbehaviors by checking the consistency between the driver's intention, the vehicles' behaviors and environment. Key point is to find an appropriate norm model for anomaly detection.
- This paper doesn't consider the situation that if one comprised ECU sends fake messages (Even the driver presses the brake pedal, the sensor sends information that's totally different from the driver's intention.)

- Other papers of author try to solve this problem, i.e. attacker identification.

[1] E. Bakker, L. Nyborg, and H. Pacejka, "Tyre modelling for use in vehicle dynamics studies," in SAE Technical paper 870421, Feb. 1987.

Sec'16 and CCS'17 are aimed at finding an effective way to fingerprint ECUs. The thus derived fingerprints are used to construct an IDS(intrusion detection system) to detect attack and identify the attacker.
The key point of building an IDS is to find a **feature** to fingerprint ECUs, which should be unique, stable and non-duplicable (at least not easy to be duplicated).

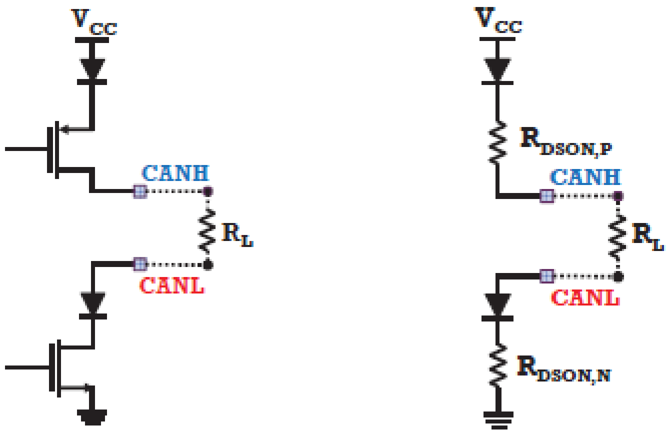
Sec' 16
Exploit message periodicity to fingerprint ECUs.

CCS' 17
The main focus of the paper is about attacker identification, not attack detection. Exploit small inherent discrepancies of CAN output voltages when sending a 0-bit to fingerprint ECUs, such constructed system called Viden.
Methods:

Viden measures the CANH&CANL voltages and maps them to the ID of the message just received. Viden exploits selected voltages that are outputted by the same message transmitter to derive a voltage instance, which can be used for reflecting the transmitter ECU's voltage output behavior.
When an attack is detected, Viden construct a voltage profile for the attack messages and maps that profile to one of those Viden has, thus identifying the attacker ECS.

The paper considers the relationship between the numbers of ECUs and IDs of messages to be 1, N. (One message only comes from one ECU.)

The paper proves that there exist some small differences between ECUs' output voltage from the perspective of transistors.



(a) Transceiver schematic. (b) When sending a 0-bit.

Figure 2: Output schematics of a CAN transceiver.

Experiment:
On a CAN bus prototype and two real vehicles (same as Sec’ 16).
Low false identification rate of 0.2%.

My conclusion:

- It’s an impressive solution. It requires professional experimental skills and advanced experiment equipment.

CCS’ 16

This paper focuses on what an adversary can do with a compromised ECU, rather than how the ECU was compromised.

The paper proposes a new important type of Denial-of-Service(DoS) attack called bus-off attack. It exploits the error-handling scheme of CAN protocol to disconnect or shut down good/uncompromised ECUs.

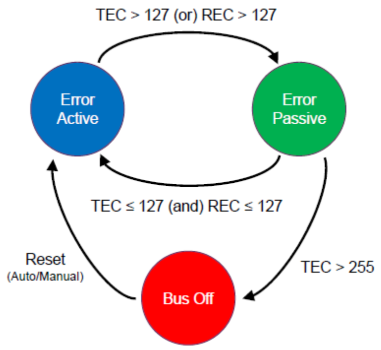


Figure 3: State diagram of fault confinement in CAN.

Error-handling scheme aims to detect errors in CAN frames and enables

ECUs to take appropriate actions, such as discarding a frame, retransmitting a frame, and raising error flags. When error occurs, the counter of node (Transmit Error Counter, Receive Error Counter) will increase. When TEC ⩾ 255, it's identified as a serious situation of disrupting bus communication, the corresponding ECU enters the Bus-off mode. Usually, the ECU is forced to shut down and not participate in sending/receiving data on the CAN bus at all.

The paper first considers an adversary is capable of performing injecting any messages with forged ID, DLC, and data on the bus.

To achieve this goal, the attacker forces the TEC of an uncompromised ECU to continuously increase by iteratively injecting attack messages, and in the end triggers the victim enters Bus-off mode, and forces the victim ECU or even the entire network to shut down.

To launch an attack, the attack message should satisfy three conditions:

1. ID – same ID as target message;
2. Timing – Transmitted at the same time as target message;
3. Contents – Having at least one bit position in which it's dominant(0), whereas it's recessive(1) in target message.

The condition 2 is the most difficult to fulfill due to the jitters in CAN messages make the actual message periodicities deviate from their preset value. The paper defines 'unique Preceded ID' of the target message, and use it to make the exact timing of message transmissions becomes rather predictable and even determinative.

Experiment:

Evaluate feasibility on a CAN bus prototype and two real vehicles (same as Sec'16 and CCS'17).