Crash Reconstruction through Digital Forensics of Vehicle Event Data Recorders

Carson Green, Dr. Jeremy Daily

Department of Systems Engineering, Colorado State University, Fort Collins, CO, USA

SYSTEMS ENGINEERING
COLORADO STATE UNIVERSITY

WALTER SCOTT, JR. COLLEGE OF ENGINEERING
COLORADO STATE UNIVERSITY

Introduction:

Most modern vehicles now contain event data recorders (**EDR**) which are used to log technical vehicle information such as: velocity, ignition cycle, fault codes, safety belt status, and more information regarding the vehicle's performance and status before/during a crash. When a collision occurs, an airbag control module (**ACM**) stores data to the electrically erasable programmable read-only memory (**EEPROM**) which in many cases is still functional even when the ACM itself is not. In chip-swapping, the EEPROM is manually removed then reinstalled onto a surrogate ACM for the purpose of extracting its data. The scope of this research is to gain more insight into methods used to retrieve EDR data through extraction/decryption, chip swapping, and the usage of the Bosch Crash Data Retrieval Tool. Altogether, these methods can be useful for crash reconstruction as it may provide evidence in legal proceedings.

Methods/Experimental Setup:

Figure 1. BOSCH Crash Data Retrieval (**CDR**) tool connected to an ACM for extraction.

Figure 2. Images of an ACM that have been damaged from a crash.

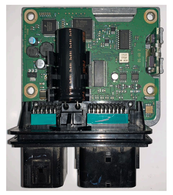


Figure 3. ACM with casing removed.

Figure 4. Closeup of an ACM microcontroller containing EEPROM: 512 Kbytes of flash memory.

Figure 5. Workstation set up with heat gun, solder iron, tools, and ACM chip being transferred.

Results:

- The chip-swap method tests data for transferability after substituting memory chips. Original data is then compared side-by-side with data after the chip-swap, showing the ignition cycle counter in **Figure 6** increase by 2 cycles. This data represents the number of times the engine starts a vehicle has experienced. The differing values are explained by the CDR tool mimicking two engine starts in order to image the data from the EEPROM, meaning no loss of integrity within the data occurred. Another chip swap test (not shown) also yielded results of 100% accurate data transfer.

```
C:\Users\student\Desktop>FC /N OriginalAC1Extraction.txt Chipswap#1_AC1-AA.txt
Comparing files OriginalAC1Extraction.txt and CHIPSWAP#1_AC1-AA.TXT
***** OriginalAC1Extraction.txt   <-- Original hexadecimal data: lines 15-17.
   15:  Event Record 1
   16:  50 43 00 00 70 43 00 00 96 6F 46 00 1A 09 00 00 D5 F0 FF FF 01 09 00 00 1F 1E 4F FF
   17:  50 7B B4 00 D7 80 FF FF B5 E0 B0 00 6F DD B0 00 BE DA B0 00 EB D7 B0 00 99 D5 B0 00
***** CHIPSWAP#1_AC1-AA.TXT   <-- Data extracted after chip swap, showing only one difference.
   15:  Event Record 1
   16:  50 43 00 00 72 43 00 00 96 6F 46 00 1A 09 00 00 D5 F0 FF FF 01 09 00 00 1F 1E 4F FF
   17:  50 7B B4 00 D7 80 FF FF B5 E0 B0 00 6F DD B0 00 BE DA B0 00 EB D7 B0 00 99 D5 B0 00
*****
```

Figure 6. (above): Hexadecimal values being compared, original data on top and data post chip-swap below.

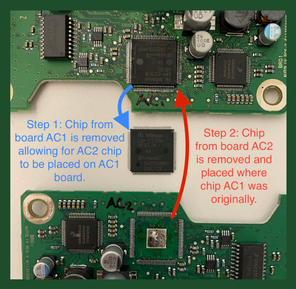
- Using a machine-in-the-middle attack, interception of the byte transfer is now possible allowing for live alteration of data as it is being imaged from the Bosch CDR tool. So far, the VIN and numerous sensor serial numbers have been altered which is reflected within a CDR report.

VIN as programmed into RCM at factory	1FMCU9EG5AKC30016
Current VIN from PCM	1FMCU9EG5AKC30016
Ignition cycle, download (first record)	11,556
Ignition cycle, download (second record)	N/A
Restraints Control Module Part Number	BL84-14B321-AA
Restraints Control Module Serial Number	7108784300000000
Restraints Control Module Software Part Number (Version)	BR33-14C028-AB
Left/Center Frontal Restraints Sensor Serial Number	125E270C
Left Side Restraint Sensor 1 Serial Number	0C8E6DAC
Left Side Restraint Sensor 2 Serial Number	0C900D1D
Right Frontal Restraints Sensor Serial Number	125D7942
Right Side Restraint Sensor 1 Serial Number	125E5DFC
Right Side Restraints Sensor 2 Serial Number	125E1165

Figure 8. (left) Original report before manipulation detailing frontal restraints serial numbers. The CAN frames were found within the diagnostic session by manual decoding.

VIN as programmed into RCM at factory	1FMCU9EG5AKC30016
Current VIN from PCM	1FMCU9EG5AKC30016
Ignition cycle, download (first record)	11,737
Ignition cycle, download (second record)	N/A
Restraints Control Module Part Number	BL84-14B321-AA
Restraints Control Module Serial Number	7108784300000000
Restraints Control Module Software Part Number (Version)	BR33-14C028-AB
Left/Center Frontal Restraints Sensor Serial Number	DEADBEEF
Left Side Restraint Sensor 1 Serial Number	DEADBEEF
Left Side Restraint Sensor 2 Serial Number	DEADBEEF
Right Frontal Restraints Sensor Serial Number	DEADBEEF
Right Side Restraint Sensor 1 Serial Number	DEADBEEF
Right Side Restraints Sensor 2 Serial Number	DEADBEEF

Figure 9. (left) Report showing the serial numbers post-alteration. This was from the same EDR and utilized a Teensy 4.0 to locate the sensor serial number data and successfully alter it.



Application of Knowledge:

The concepts and skills of gathering, decoding, and understanding the data from EDR units have given me a strong foundation for beginning a career in vehicle cybersecurity. I plan to continue my research by applying these skills to securing and understanding more about the challenges faced by the industry of vehicle cybersecurity. By learning new concepts, I have begun to appreciate how valuable my skills are in using them to defend the network of a car and plan to continue doing so.

Discussion/Next Steps:

Moving forward, altering data such as vehicle speed or seatbelt status could yield interesting results within the field of crash reconstruction and can pose a risk to the integrity of evidence presented in a court case. By changing the vehicle's operation data presented within a CDR report, the outcome of a trial could change completely. Another topic of research that is being looked into is how to validate this data to ensure no changes have occurred.

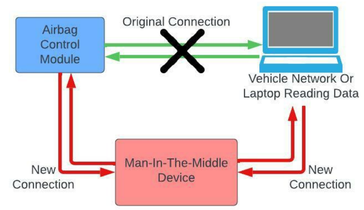


Figure 9. Diagram of a machine-in-the-middle (MITM) attack between an ACM and the diagnostic tool.

Conclusions:

Chip swapping has provided 100% accuracy of data transfer by swapping a microcontroller from a damaged EDR onto a surrogate and maintaining the original state. As long as no device has manipulated the data being imaged, the method of chip-swapping can provide essential data used in crash reconstruction/forensics as it becomes more widely accepted; additionally, it may even be used as evidence in legal proceedings given the data is unaltered.

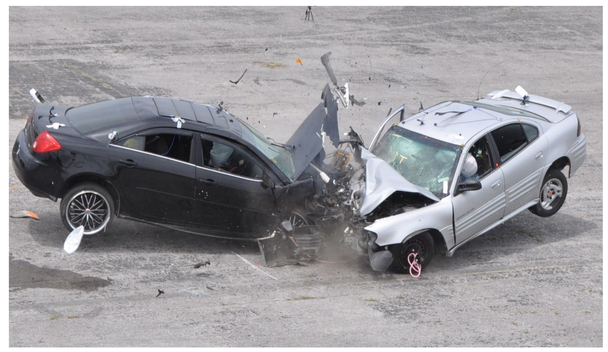


Figure 11. Image of a staged crash where an ACM could get damaged (J. Daily photograph)..

SURE Experience Benefits:

Participating in this research alongside helpful mentors has increased my motivation and passion for engineering. The ability to learn from people more knowledgeable in the field, especially those who are willing to help is a great way to gain more interest and truly enjoy the work. The opportunity to work at a location like the Powerhouse Energy Institute makes the work I am doing seem much more memorable. Research is challenging; however, it provides priceless learning experiences and applicable skills which I will use not only in my professional career, but also in my personal life. Special thanks to Susan Benzel, Dixie Poteet, Dr. Daily, David Nnaji, and team members of the Systems Cyber team for their help and guidance throughout this research.

References and Acknowledgements:

[1] Daily, J., DiSogra, M., and Van, D., "Chip and Board Level Digital Forensics of Cummins Heavy Vehicle Event Data Recorders," *SAE Int. J. Adv. & Curr. Prac. in Mobility* 2(4):2374-2388, 2020, https://doiorg.ezproxy2.library.colostate.edu/10.4271/2020-01-1326.

[2] Ruth, R. R., & Daily, J. (2014). Accuracy and timing of 2013 Ford Flex Event Data Recorders. *SAE Technical Paper Series*. https://doi.org/10.4271/2014-01-0504.

Thank you to the Suzanne and Walter Scott Foundation, The Filsinger Family, and Contributors to the Dean's Innovation fund for making the SURE program possible.