Hochschule Karlsruhe
Technik und Wirtschaft
UNIVERSITY OF APPLIED SCIENCES

Technische Universität München

Vulnerability in pyrotechnical control units of passenger cars

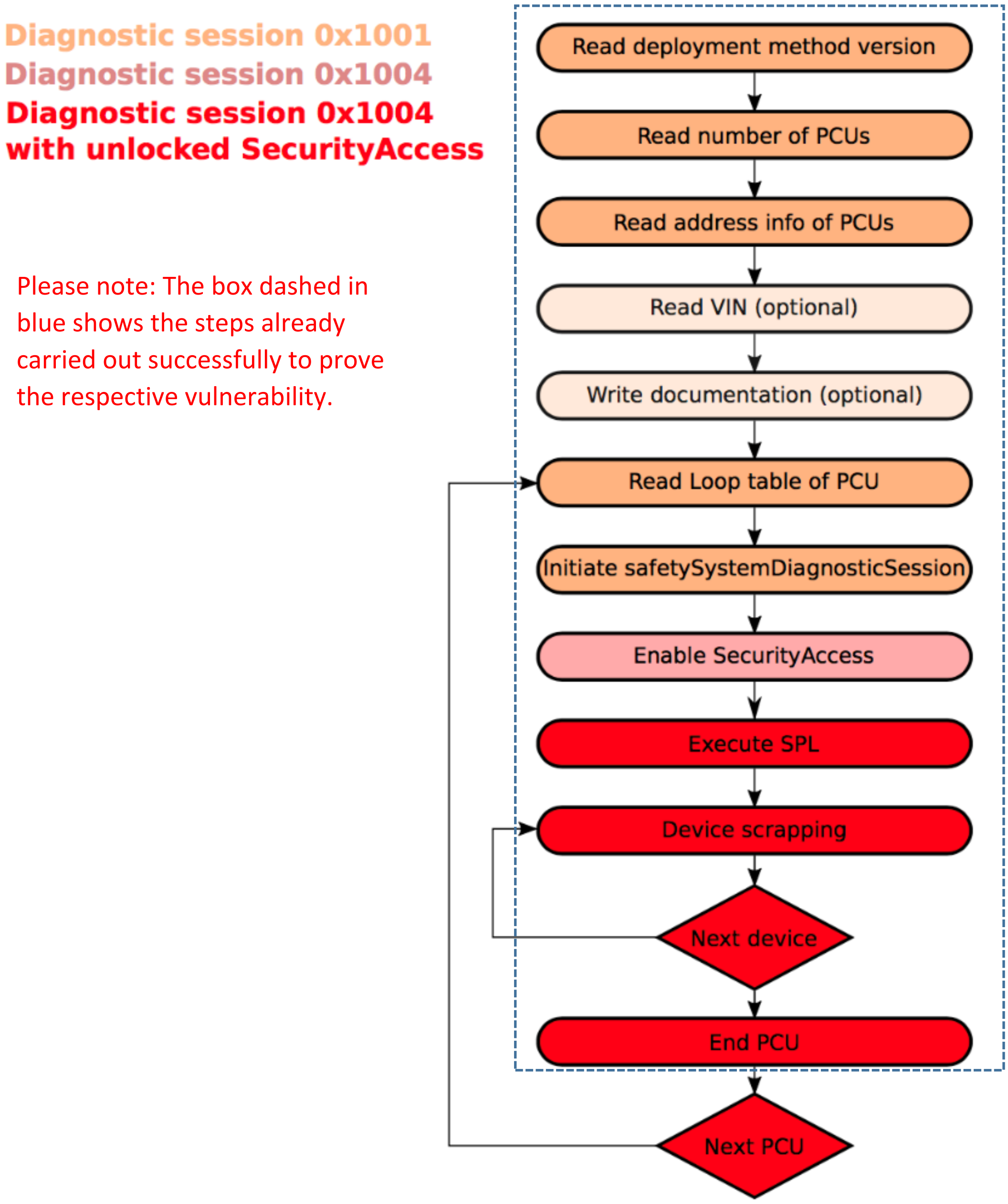
I. Vulnerability description

Threat:	Physical injury of passengers by willful detonation[1] of pyrotechnical charges while the vehicle is not moving
Affected component:	Airbag control units (pyrotechnical control units (PCUs)) implemented complying with the ISO standard 26021 (*End-of-life activation of on-board pyrotechnic devices*)
Vulnerability description:	1. According to the ISO standard 26021 the security access represents the only protection against unauthorized detonation of pyrotechnical charges. The seed and key pair required for the security access (SA) (see figure 1) is calculated by means of a weak algorithm (key by complementation) complying with the ISO 26021. This ISO standard gives the impression that the description of the SA is not only an example for an algorithm but a binding requirement. Thus, we suppose that several manufacturers copied the respective SA algorithm from the standard and implemented it without any alteration. This enables an attacker to calculate the proper key for the SA if s/he has the ISO 26021 available. In addition to the above-mentioned vulnerability also a brute-force attack can cause the detonation of the airbag even if the key algorithm is not known. Such an attack can be made by means of a script within a short period of time: 2. The ISO 26021 proposes to use a 2-byte key which results in 65536 different key pairs to be checked by an attacker in case s/he does not know the algorithm. Furthermore, the ISO standard states the following: “There is no time period which needs to be inserted between access attempts”. Already these two weaknesses facilitate a brute-force attack on the SA seed and key pair. Additionally, the ISO 26021 requires that byte 1 of the only 2-byte-long seed includes the definite version number (0x01) of the implemented load detonation method. This means that the first byte of the seed is known and the

[1] We would like to point out that a successful detonation was possible. However, the detonation was not carried out in a vehicle but in a test setup. This setup consisted of an airbag control unit and resistors which emulated the detonators. Additionally, we emulated the CAN bus traffic by recording and replaying messages of a real vehicle.

	resultant seed and key pairs are reduced from 65536 to only 256 possible pairs.
Precondition:	1. The airbag control unit was implemented in compliance with the ISO 26021 2. Access to the OBD connector or the internal CAN bus used for sending the OBD messages Assumed precondition: 3. The ignition of the vehicle has to be turned on (corresponds to terminal 15) and the speed of the vehicle has to be less than 6 km/h. Please note: We have detected the respective vulnerability only in passenger cars manufactured from 2014 onwards.
Technical contact:	**Johannes Braun, Jürgen Dürrwang M.Sc.** Karlsruhe University of Applied Sciences Institute of Energy Efficient Mobility Moltkestr. 30 76133 Karlsruhe Phone: +49(0) 721/925 – 1432 E-mail: juergen.duerrwang@hs-karlsruhe.de
Administrative contact:	**Prof. Dr.-Ing. Reiner Kriesten** Karlsruhe University of Applied Sciences Institute of Energy Efficient Mobility Moltkestr. 30 76133 Karlsruhe Phone: +49(0) 721/925 - 1747 E-mail: reiner.kriesten@hs-karlsruhe.de
	Prof. Dr. Alexander Pretschner Technical University of Munich Informatics 22 - Chair of Software Engineering Boltzmannstr. 3(5611)/I 85748 Garching Phone: +49 (89) 289 – 17876 E-mail: alexander.pretschner@tum.de
Funding: Bundesministerium für Bildung und Forschung	The above-mentioned research results are part of the SAFE ME ASAP project (number 03FH011IX5) funded by the German Federal Ministry of Education and Research (BMBF).

II. Appendix


Diagnostic session 0x1001
Diagnostic session 0x1004
Diagnostic session 0x1004 with unlocked SecurityAccess
Read deployment method version
Read number of PCUs
Read address info of PCUs
Read VIN (optional)
Write documentation (optional)
Read Loop table of PCU
Initiate safetySystemDiagnosticSession
Enable SecurityAccess
Execute SPL
Device scrapping
Next device
End PCU
Next PCU

Please note: The box dashed in blue shows the steps already carried out successfully to prove the respective vulnerability.

Figure 1: Procedure leading to a detonation of the pyrotechnical units complying with the ISO standard 26021 [1].

References

[1] 26021-3:2009. 05.2009. *Road vehicles -- End-of-life activation of on-board pyrotechnic devices*