2022-01-0132 Published 29 Mar 2022

UDS Security Access for Constrained ECUs

Martin Thompson ZF Automotive UK Ltd

Citation: Thompson, M., "UDS Security Access for Constrained ECUs," SAE Technical Paper 2022-01-0132, 2022, doi:10.4271/2022-01-0132.

Received: 24 Jan 2022 Revised: 24 Jan 2022 Accepted: 13 Jan 2022

Abstract

Legacy electronic control units are, nowadays, required to implement cybersecurity measures, but they often do not have all the elements that are necessary to realize industry-standard cybersecurity controls. For example, they may not have hardware cryptographic accelerators, segregated areas of memory for storing keys, or one-time programmable memory areas. Such systems must still be protected with a sufficient level of rigor against attackers who wish to modify their operation or extract confidential information from them. A critical interface to defend is the Unified Diagnostics Service (UDS) interface which is used in many areas across the whole vehicle lifecycle. While the UDS service $27 (Security Access) has a reputation for poor cybersecurity, there is nothing inherent in the way it operates which prevents a secure access-control from being implemented. This paper describes an approach to providing UDS Security Access within systems which have very constrained processors (in terms of processing power, memory size and, in particular, cybersecurity features) which can be applied to multiple vehicles across many manufacturers. It describes, in detail, methods for generating UDS-Seeds and UDS-Keys in the absence of a hardware security module (HSM) with a true-random number generator, and without use (by the user who is requesting access) of IT-infrastructure. In addition, the problem of key-management and distribution is tackled head-on and not left as an implementation detail. A threat analysis has been performed (according to ISO/SAE 21434) using model-based tools, the results of which are presented in this paper. The constraints (some of which make it difficult to properly secure certain key material) result in risks which become clear in the threat analysis. Potential future users of this scheme can use this analysis to assess the residual risks in their own applications.

Introduction

Electronic control units on vehicles provide interfaces which can modify the content ECU in ways which may compromise the safety, emissions or other critical behaviors of the vehicle. As vehicles develop, in particular to future hybrid powertrains, the breadth of these functions will only get greater [1]. It is clear that such access must be controlled to allow only authorized users to execute these diagnostic functions [2].

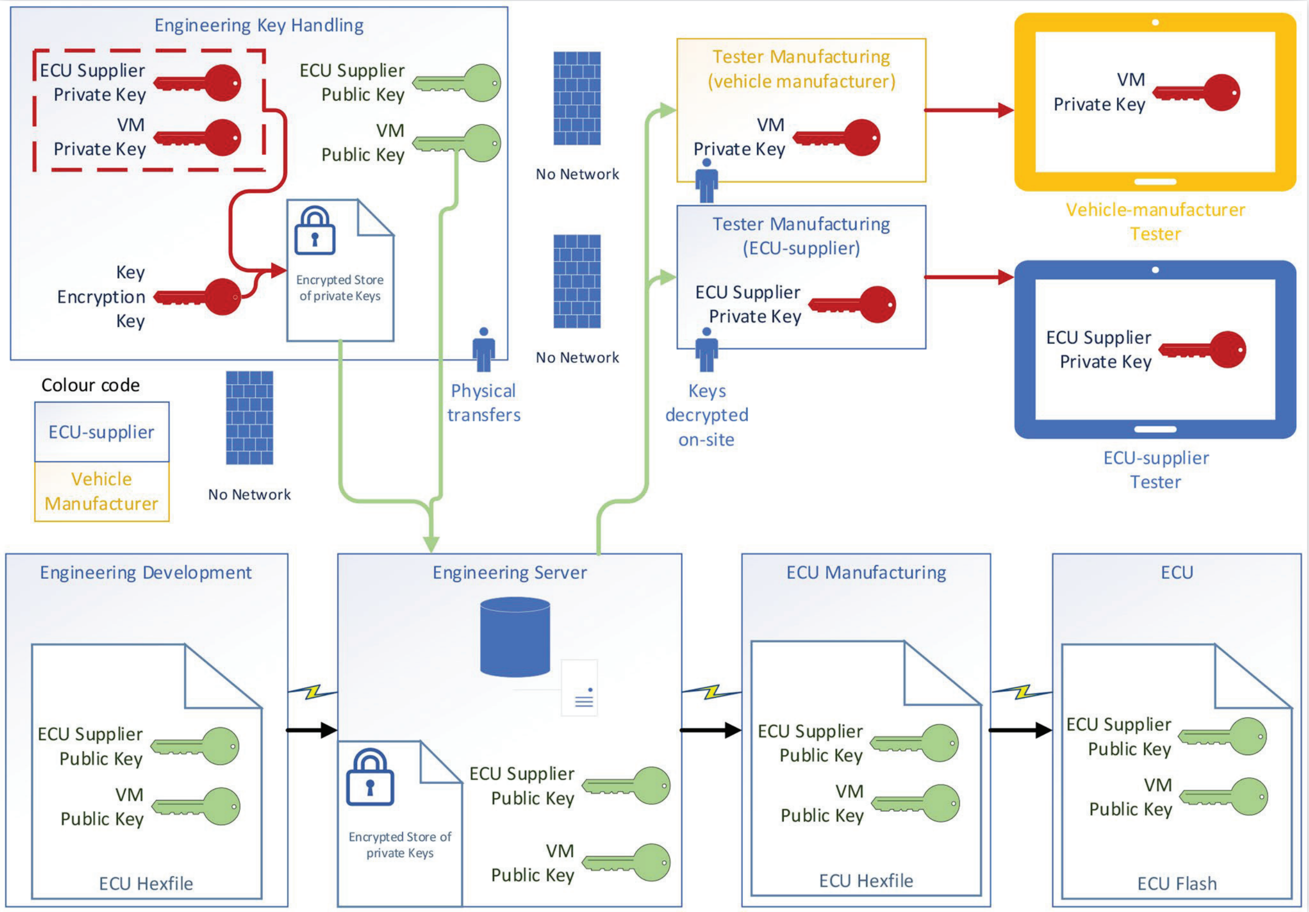
The Unified Diagnostics Services (UDS) protocol stack is used to provide networked access to diagnostic services on all modern Electronics Control Units (ECUs). It can operate using a variety of physical interfaces (for example, CAN, Ethernet) but the fundamental protocol remains the same. UDS is documented within the ISO standard documents in the ISO14229 series. UDS Security Access (Service $27) is intended to restrict "access for security, emissions, or safety reasons" [2]. It provides a standard challenge/response structure - the actual implementation (i.e. the form of the challenge and the response) is not specified. In the 2020 revision of the ISO14229 specification, UDS Authenticated Access (Service $29) was added, which standardizes certificate-based asymmetric authentication methods, but places larger demands relating to the infrastructure required to authenticate users.

UDS provides multiple "levels" of Security Access. At the base level, anyone with access to the tools (which are publicly available) can gain access to the ECU. This base level does not provide any security, so only a small set of functions should be provided at this level. When other security levels are activated, only one can be active at any given time. The "meaning" of the levels of security access, and therefore which privileges are enabled, is embedded within the software of the ECU.

When legacy ECUs units are required to implement cybersecurity measures, they often do not have all the facilities that would be expected and are necessary to implement industry-standard cybersecurity controls.

This paper describes a design-pattern by which legacy control units can provide a reasonable level of UDS-based cybersecurity, working within the constraints often encountered within such systems. We present these constraints, and a realistic threat model which is applied. A detailed description of the system and notes on the implementation are also presented. This is followed by a summary of the threat analysis that has been performed. It should be noted that there exists a tension between enabling legitimate mechanics access to potentially harmful functions (for example, those covered by 'right-to-repair' legislation, amongst others) and stopping attackers from doing damage. This paper does not offer a

FIGURE 2 block diagram of the key interactions



A threat analysis has been performed and can be used by implementors as part of their "whole ECU" threat analysis efforts.

A future implementation could extend this work to defend the tester keys more effectively. This could be achieved by provisioning them into a local Trusted Platform Module, within the tester, or to a smart card which could be inserted into the tester. This would make it more difficult for an attacker to extract the key and clone their own testers.

References

1. Zhu, D., Pritchard, E., Reddy Dadam, S., Kumar, V. et al., "Optimization of Rule-Based Energy Management Strategies for Hybrid Vehicles Using Dynamic Programming," *Combustion Engines* 184 (2021).
2. ISO, "ISO 14229-1:2020 Road Vehicles—Unified Diagnostic Services (UDS)—Part 1: Application Layer," 2020, https://www.iso.org/standard/72439.html.
3. Wikipedia, "Challenge-Response Authentication," https://en.wikipedia.org/wiki/Challenge%E2%80%93response_authentication.
4. Yubico, "U2F Technical Overview," accessed September, 2021, https://developers.yubico.com/U2F/Protocol_details/Overview.html.
5. NIST, "FIPS180-4—Secure Hash Standard (SHS)," 2015, https://csrc.nist.gov/publications/detail/fips/180/4/final.
6. NIST, "SP 800-90A—Recommendation for Random Number Generation Using Deterministic Random Bit Generators," 2015, https://csrc.nist.gov/publications/detail/sp/800-90a/rev-1/final.
7. Microsoft, "Bitlocker Overview," accessed August 2021, https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview.
8. Basel Committee on Banking Supervision, "Core Principles for Effective Banking Supervision," December 15, 2019, accessed October 2021, https://www.bis.org/basel_framework/chapter/BCP/01.htm?inforce=20191215&published=20191215.
9. NIST, "SP800-57 Recommendation for Key Management (rev5)," 2020.
10. FIDO Alliance, 2017, Accessed September 2021, https://fidoalliance.org/specs/fido-u2f-v1.2-ps-20170411/fido-u2f-overview-v1.2-ps-20170411.pdf.
11. IETF, "PKCS #1: RSA Cryptography Specifications Version 2.2," November 2016, accessed November 2019, https://tools.ietf.org/html/rfc8017.

12. IEEE/SAE, "ISO/SAE 21434 Road Vehicles—Cybersecurity Engineering," 2021, accessed October 2021, https://www.iso.org/standard/70918.html.

13. Garcia, F. and Van den Herrewegen, J., "Beneath the Bonnet: A Breakdown of Diagnostic Security," 2018, Accessed October 2021, https://www.cs.bham.ac.uk/~garciaf/publications/BtB.pdf.

14. NIST, "SP 800-38D—Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC," https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf.

Contact Information

Martin Thompson
martin.j.thompson@zf.com

Acknowledgments

The author is very grateful to his colleagues for their help with the development of this protocol and in reviewing this paper: Andrew Bold, Michael Feiri, Gurchetan Grewal, Thorsten Hestermeyer. In addition, the author thanks the anonymous reviewers for their valuable input. Any remaining errors and omissions, of course, remain the author's.

Definitions/Abbreviations

CAN - Controller Area Network

CSPRNG - Cryptographically Strong Pseudo Random Number Generator

DID - Data Identifier

ECU - Electronic Control Unit

HSM - Hardware Security Module

TARA - Threat Analysis and Risk Assessment

TRNG - True Random Number Generator

UDS - Unified Diagnostics Services

VM - Vehicle Manufacturer

Appendix

Block Diagram

(Block Diagram.png is supplied separately in high resolution)

Residual Risks

Risk	Risk level with no controls	Residual Risk Level after controls	Risk Treatment	Controls
R.1: Tampering - ECU and its environment	5	3	Reduction	C.1, C.2, C.6
R.3: Information Disclosure - ECU supplier Tester	4	3	Reduction	C.11
R.4: Attacks using the tester messages	5	1	Reduction	C.3, C.4, C.5
R.5: Elevation of privilege within ECU	5	1	Reduction	C.7
R.6: Attacks on Production Line	1	1	Reduction	C.9
R.7: Attacks on Engineering Servers	1	1	Reduction	C.9
R.8: Attacks on development stations	1	1	Reduction	C.9
R.9: Information Disclosure - VM Tester	2	2	Acceptance	No further reasonably practical mitigations possible
R.10: Attacks on Key Handling stations	4	3	Reduction	C.10
R.11: Information Disclosure of the Key Encryption Key	4	3	Reduction	C.11