Response to Reviewers' Comments

Paper title: Designing and Implementing an AUTOSAR-based Basic Software Module for Enhanced Security

Authors: G. Bella, P. Biondi, G. Costantino, I. Matteucci

First of all, we would like to thank the editor and the reviewers for their time, their valuable comments and their insightful suggestions. Taking into account the issues raised by the reviewers, we modified our manuscript. Below you find the response to the specific comments of each reviewer.

Please note that all amendments to the paper are highlighted in red and in blue. The red part are referred to our amendments of first round comments, while the blue one are referred to all amendments of the new valuable comments of reviewers. We also attach the paper diff between the second and third submission.

Reviewer 1. *The authors have addressed my questions, I have no further inquiries.*

We would like to thank the reviewer. It is a pleasure to know that we have responded satisfactorily to all the valuable comments provided by this reviewer in the previous round of review.

Reviewer 2. *In this revision, the authors have expanded the section dedicated to the comparison with the related work, identifying various aspects on which different solutions are evaluated. The proposed work does seem to provide an additional trade-off points compared to the related work, according to the table, although not all aspect may be relevant to all implementations.*

We would like to thank the reviewer. It is a pleasure to know that we have updated satisfactorily the related work section as requested by this reviewer.

Q1 *On the other hand, as far as I can tell, the rest of the paper is largely unchanged. Therefore my original concern regarding the limited extension over the previous conference publication still stands.*

A1 We would like to thank the reviewer that prompted us to reorganise the paper to better highlight the innovative aspects of our research. Thus, in this revised paper submission, we have deeply reorganised the paper, in particular, the paper structure has been revised as following:

- The background section has been removed. This help us to highlight the CINNAMON requirements and specification are not related to a particular communication protocol
- The part dealing with the specification of CINNAMON and its Security Profiles with the implementation one are balanced.
- At the beginning of Section 6, we clearly explain that only the CINNAMON implementation has been customised for the CAN bus protocol.
- Section 7 and Section 8 have been merged in a unique section (Section 7) about the security profiles implementation. In the new version of Section 7 we maintain the description of crucial details and some part of the code highlighting the difference between the sender and receiver code.

Moreover, to clearly show the changes that we have done following the two rounds of re-submission of the paper, we have attached to this submission an additional version of our paper in which we coloured in red the changes applied compared to the first revision, and in blue how we amended the paper according to the comments for the second revision.

Q2 *In particular, while I agree that the implementation details are unpublished, my point is that they do not add scientifically to the paper, since the reader can very easily imagine how the whole system can be implemented.*

A2 Thanks to the reviewer for the comment. We agree that the implementation is the natural consequence of CINNAMON and that the reader can image this result. However, although the implementation may seem like a trivial process, it is also true that we have chosen to run the implementation on boards resembling the ones deployed into vehicle to get as close as possible to the ECUs of modern cars. Furthermore, this implementation does not turn out to be a trivial and immediate task since the targeted boards have limited computational power and memory limits. This point increases the effort required in the implementation and despite the limitations of the boards it is possible to obtain promising performance aspects that match automotive protocols requirements.Furthermore, for years the automotive field has been pushing on the implementation factor as we try to speed up the process of introducing security and safety into cars. However, we have reorganised our manuscript to orient it more on CINNAMON design aspects than implementation ones.

Q3 *The performance results are similar to those shown in the conference publication.*

A3 We would like to thank the reviewer for this comment. In Section 8 of the current version of the paper, we highlighted the main differences between the results we present in this paper and in the conference one.

In our preliminary work [6], we provided a first quantitative evaluation of a CAN-based protocol. In [6], we presented the performance evaluation of a single one profile, i.e., Profile 1, that was designed and implemented in a different way to establish the MAC and frame encryption w.r.t. what is shown in Section 5.1. Therefore, we improved the CINNAMON design by choosing different encryption algorithms, MAC and freshness and this has allowed us to obtain better computation results related to Profile 1.

With this new paragraph, we have highlighted the differences for two main reasons: 1) we aim to demonstrate that CINNAMON is viable and promising in terms of performance and 2) the current implementation has differences

compared to the previous version that improve its performance.

Q4 *If the implementation had run under the AUTOSAR framework, at least it would be a strong validation of its integration, but this is not the case. Besides, as far as I can tell, the new revision does not mention that the implementation is not running under AUTOSAR, which could be misleading.*

A4 We are sorry for not clearly having expressed how our implementation is link with the AUTOSAR framework. Concerting this aspect, we would like to say that our goal through CINNAMON is to design and build a single module that is ready to be integrated with the AUTOSAR framework. In fact, the framework is designed with a modular approach in which each module aims to perform a particular functionality. In the design and implementation of CINNAMON, we decided to create a Basic Software Module that correctly fits the requirements of the framework to seamlessly work with the other modules. This means that although in the presented implementation of CINNAMON we did not implemented all the AUTOSAR framework modules too, our CINNAMON BSW has been implemented to work with them.

To express this concept, at the beginning of Section 4, we wrote:

> The CINNAMON module is a Basic Software (BSW) module capable of protecting on-board CAN Bus communications and is based on AUTOSAR in the sense that it extends AUTOSAR in terms of possible functionalities provided and can be integrated into the current AUTOSAR architecture. Moreover, CINNAMON is designed as a single module that is built to provide security functionalities within the AUTOSAR framework. Thus, it is designed and implemented (Section 6 and Section 7) to work with the other modules already present into the AUTOSAR Classic Platform.

Moreover, to better clarify this point related to CINNAMON and how it can be run into the AUTOSAR framework, we wrote two new sections in the current version of the paper.

Section 4.1, titled "Integration with AUTOSAR", contains Figure 1, which was already present in the previous version of this paper, and its goal is to discuss how CINNAMON BSW design is fully integrated into the AUTOSAR

framework. In particular, we wrote that:

> More specifically, the PDU Router module provides services for routing Protocol Data Units between modules such as the communication and transport modules. As for the Crypto Service Manager, it provides services to allow single access to basic cryptographic functionality for all software modules. Hence, CSM provides a standardised interface at the software levels to access these features. Since CINNAMON is based on AUTOSAR, it is able to use other AUTOSAR components to carry out communication and security operations.

Also in Section 6.1, titled "Testbed resembling AUTOSAR Classic Platform", we clarify how our implementation of CINNAMON BSW can be integrated with the AUTOSAR framework.

> In order to resembling the architecture of the AUTOSAR Classic Platform, we set up our testbed consisting of two ECUs and a laptop interconnected via CAN bus. The laptop can send and receive frames in the channel, which can in turn be connected to other networks, for example also through the PDU Router, as in modern automotive networks.

And:

> We can therefore conjecture that all cryptographic operations require interaction with the Crypto Service Manager that provides the ECU the needed cryptographic keys.

Q5 *I'm not sure I understand the difference between AUTOSAR compliance and being based on AUTOSAR. What are the implications?*

A5 In the following we, try to explain the difference between AUTOSAR compliance and AUTOSAR based. Specifically in the first case, being Compliant with AUTOSAR means that the proposed module has passed a rigorous compliance process to be possibly integrated within the framework. On the other hand, being AUTOSAR based means that the proposed module has been designed and implemented according to the guidelines drawn by AUTOSAR but it is not yet declared compliant.

In this regard, we have included this sentence in the paper:

The CINNAMON module is a Basic Software (BSW) module capable of protecting on-board CAN Bus communications and is based on AUTOSAR in the sense that it extends AUTOSAR in terms of possible functionalities provided and can be integrated into the current AUTOSAR architecture. Moreover, CINNAMON is designed as a single module that is built to provide security functionalities within the AUTOSAR framework. Thus, it is designed and implemented (Section 6 and Section 7) to work with the other modules already present into the AUTOSAR Classic Platform.