

Accepted Manuscript

Building an automotive security assurance case using systematic security evaluations

Madeline Cheah, Siraj A. Shaikh, Jeremy Bryans, Paul Wooderson

PII: S0167-4048(18)30358-4
DOI: [10.1016/j.cose.2018.04.008](https://doi.org/10.1016/j.cose.2018.04.008)
Reference: COSE 1330



To appear in: *Computers & Security*

Received date: 15 August 2017
Revised date: 26 March 2018
Accepted date: 9 April 2018

Please cite this article as: Madeline Cheah, Siraj A. Shaikh, Jeremy Bryans, Paul Wooderson, Building an automotive security assurance case using systematic security evaluations, *Computers & Security* (2018), doi: [10.1016/j.cose.2018.04.008](https://doi.org/10.1016/j.cose.2018.04.008)

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

Building an automotive security assurance case using systematic security evaluations

Madeline Cheah^a, Siraj A. Shaikh^b, Jeremy Bryans^b, Paul Wooderson^a

^a*HORIBA MIRA, Nuneaton, CV10 0TU, United Kingdom*

^b*Research Institute for Future Transport and Cities, Coventry University, CV1 5FB, Coventry, United Kingdom*

Abstract

Security testing and assurance in the automotive domain is challenging. This is predominantly due to the increase in the amount of software and the number of connective entry points in the modern vehicle. In this paper we build on earlier work by using a systematic security evaluation to enumerate undesirable behaviours, enabling the assignment of severity ratings in a (semi-) automated manner. We demonstrate this in two case studies; firstly with the native Bluetooth connection in an automotive head unit, and secondly with an aftermarket diagnostics device. We envisage that the resulting severity classifications would add weight to a security assurance case, both as evidence and as guidance for future test cases.

Keywords: automotive, Bluetooth, cybersecurity, security assurance, penetration testing

1. Introduction

Historically, embedded systems were designed to operate in tightly-controlled environments which required specialist knowledge to design, calibrate and deploy. Developments in functionality and connectivity, however, have meant that the amount of software and its concomitant complexity has increased dramatically.

There are several trends which have contributed to the automotive threat landscape, each of which lead to increased attack surface area and increased

Download English Version:

<https://daneshyari.com/en/article/6883872>

Download Persian Version:

<https://daneshyari.com/article/6883872>

[Daneshyari.com](https://daneshyari.com)