**D5.4 Appendix G**

**Impact Analysis - Vertical 1 - Scenario 2**

|  |  |
| --- | --- |
| **Project number** | **830892** |
| **Project acronym** | **SPARTA** |
| **Project title** | **Strategic programs for advanced research and technology in Europe** |
| **Start date of the project** | **1st February, 2019** |
| **Duration** | **36 months** |
| **Programme** | **H2020-SU-ICT-2018-2020** |

|  |  |
| --- | --- |
| **Deliverable type** | Report |
| **Deliverable reference number** | SU-ICT-03-830892 / D5.4 / V1.0 / Appendix G |
| **Work package contributing to the deliverable** | WP5 |
| **Due date** | Jan 2022 – M36 |
| **Actual submission date** | 2nd February, 2022 |

|  |  |
| --- | --- |
| **Responsible organisation** | **CETIC** |
| **Editor** | Sébastien Dupont |
| **Dissemination level** | **PU** |
| **Revision** | **V1.0** |

|  |  |
| --- | --- |
| **Abstract** | Proposal of impact analysis for incremental certification in the automotive firewall update scenario |
| **Keywords** | **Impact Analysis report, Firewall, Automotive, Certification** |

**Editor**

Sébastien Dupont (CETIC)

**Contributors** (ordered according to beneficiary numbers)

Guillaume Ginis, Philippe Massonet (CETIC)

Mirko Malacario, Claudio Porretti (LEO)

**Reviewers** (ordered according to beneficiary numbers)

Maximilian Tschirschnitz (TUM)

Rimantas Zylius (L3CE)

**Disclaimer**

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the author`s view – the European Commission is not responsible for any use that may be made of the information it contains. The users use the information at their sole risk and liability.

**Executive** **Summary**

This document provides a sample impact analysis report for CAPE connected cars “Firewall update” demonstration scenario (Vertical 1 - Scenario 2). In this scenario, a new version of the firewall is available and needs to be deployed on platoon vehicles. From the certification point of view, if some certified requirements are impacted then the new firewall version must be re-certified on vehicles.

The document describes the change (firewall update), and the modifications to the affected developer evidences.

**Table of Content**

[Executive Summary 2](#_Toc121907585)

[Table of Content 3](#_Toc121907586)

[List of Figures 4](#_Toc121907587)

[List of Tables 4](#_Toc121907588)

[Chapter 1 Introduction 1](#_Toc121907589)

[Chapter 2 Description of the change(s) 3](#_Toc121907590)

[Chapter 3 Affected developer evidence 5](#_Toc121907591)

[3.1 Impact of the changes on the Security Target 7](#_Toc121907592)

**List of Figures**

[Figure 1: Target of evaluation 1](#_Toc121907579)

[Figure 2: details of the firewall component of the TOE 1](#_Toc121907580)

**List of Tables**

[Table 1: Main TOE Changes 2](#_Toc121907575)

[Table 2: Extract of Security Functional Requirements (SFRs) 7](#_Toc121907576)

[Table 3: Requirements per component of the TOE 8](#_Toc121907577)

[Table 4: Impacted requirements 9](#_Toc121907578)

# Introduction

In the SPARTA CAPE Vehicle to Infrastructure (V2I) firewall update scenario, a new version of the firewall is available and needs to be deployed on platoon vehicles. The update is performed when vehicles are not being driven. From the certification point of view, if some certified requirements are impacted then the new firewall version must be re-certified on vehicles. This requires following the certification process for the impacted parts.

**For the purpose of this demonstration, the assumption is that we base this impact analysis on preexisting accepted impact analysis reports and associated certification.**

The TOE is composed of the platooning software (SafSecPMM) and the firewall that are installed in platoon members as described in Figure 1 below.

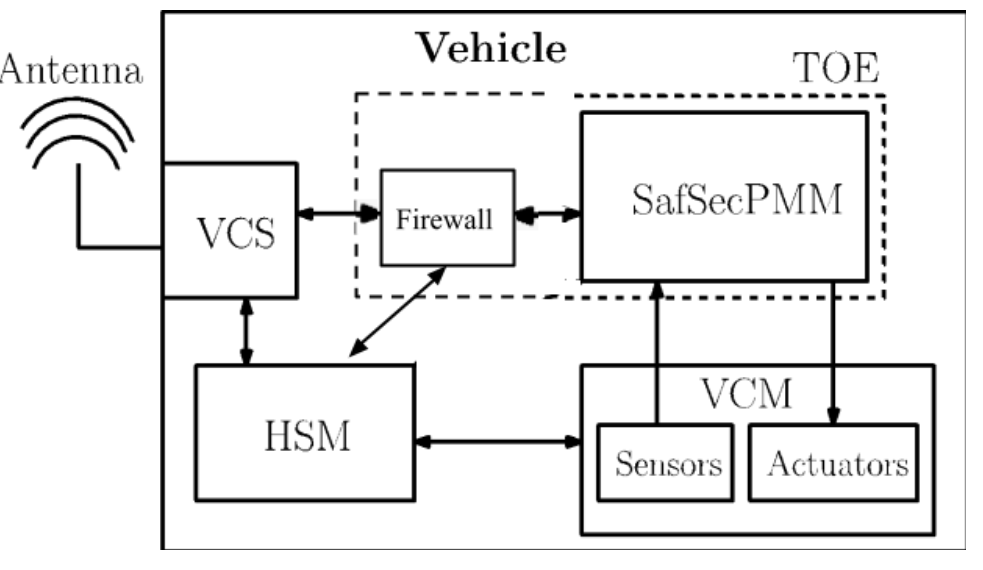


Figure 1: Target of evaluation

The firewall TSF (TOE Security Function) is composed of the green modules in Figure 2.

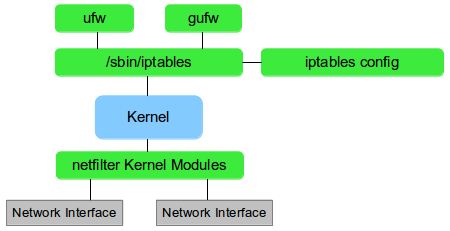


Figure 2: details of the firewall component of the TOE[[1]](#footnote-1)

The configuration controls identifiers of the TOE are shown in the following Table 1.

|  |  |
| --- | --- |
| **Evaluated Configuration (current)** | **Updated TOE Version (changes)** |
| iptables - version 1.8.6 - 2020-10-31 | iptables - version 1.8.7 - 2021-01-15 |
| SafSecPMM - version x.y.z | SafSecPMM - version x.y.z (no changes) |

Table 1: Main TOE Changes

# Description of the change(s)

The following changes to the certified product are identified: the version of the Firewall component has been updated[[2]](#footnote-2). The release notes below describe the changes for the new version of the firewall, with the associated author:

Florian Westphal (4):

[xtables-monitor: fix rule printing](https://git.netfilter.org/iptables/commit/?id=07af4da52ab3002c9cb510863b4eb7aaca4fb43b)

[xtables-monitor: fix packet family protocol](https://git.netfilter.org/iptables/commit/?id=946923b640afc2249cf98743ff60a97291108701)

xtables-monitor: print packet first

xtables-monitor:

Pablo Neira Ayuso (2):

tests: shell: update format of registers in bitwise payloads.

configure: bump version for 1.8.7 release

Phil Sutter (21):

[nft: Optimize class-based IP prefix matches](https://git.netfilter.org/iptables/commit/?id=323259001d617ae359430a03ee3d3e7f107684e0)

ebtables: Optimize masked MAC address matches

tests/shell: Add test for bitwise avoidance fixes

ebtables: Fix for broken chain renaming

iptables-test.py: Accept multiple test files on commandline

iptables-test.py: Try to unshare netns by default

libxtables: Extend MAC address printing/parsing support

xtables-arp: Don't use ARPT\_INV\_\*

xshared: Merge some command option-related code

tests/shell: Test for fixed extension registration

extensions: dccp: Fix for DCCP type 'INVALID'

[nft: Fix selective chain compatibility checks](http://git.netfilter.org/iptables/commit/?id=694612adf87fb614f16a2b678f32745d5c9d7876)

nft: cache: Introduce nft\_cache\_add\_chain()

nft: Implement nft\_chain\_foreach()

nft: cache: Move nft\_chain\_find() over

nft: Introduce struct nft\_chain

nft: Introduce a dedicated base chain array

nft: cache: Sort custom chains by name

tests: shell: Drop any dump sorting in place

nft: Avoid pointless table/chain creation

tests/shell: Fix nft-only/0009-needless-bitwise\_0

**source: IPTables 1.8.7 changelog**[[3]](#footnote-3)

Four changes in particular will be studied in this Impact Analysis Report (IAR) but the same process should be followed for all the changes.

Here is the description of these changes :

1. [xtables-monitor: fix rule printing](https://git.netfilter.org/iptables/commit/?id=07af4da52ab3002c9cb510863b4eb7aaca4fb43b): trace\_print\_rule does a rule dump. This prints unrelated rules in the same chain. Instead the function should only request the specific handle. Furthermore, flush output buffer afterwards so this plays nice when output isn't a terminal.
2. [xtables-monitor: fix packet family protocol](https://git.netfilter.org/iptables/commit/?id=946923b640afc2249cf98743ff60a97291108701): This prints the family passed on the command line (which might be 0). Print the table family instead.
3. [nft: Optimize class-based IP prefix matches](https://git.netfilter.org/iptables/commit/?id=323259001d617ae359430a03ee3d3e7f107684e0): Payload expression works on byte-boundaries, leverage this with suitable prefix lengths. (discussion)
4. [nft: Fix selective chain compatibility checks](http://git.netfilter.org/iptables/commit/?id=694612adf87fb614f16a2b678f32745d5c9d7876): Since commit 80251bc2a56ed ("nft: remove cache build calls"), 'chain' parameter passed to nft\_chain\_list\_get() is no longer effective. Before, it was used to fetch only that single chain from kernel when populating the cache. So the returned list of chains for which compatibility checks are done would contain only that single chain. Re-establish the single chain compat checking by introducing a dedicated code path to nft\_is\_chain\_compatible() doing so.

No changes to the development environment of the certified ToE have been identified.

# Affected developer evidence

Regarding the changes to the product, and according to the Common Criteria Assurance Continuity (see [8]), it is necessary to answer the following question to evaluate the affected developer evidence.

* Has it affected the Security Target?
* Has it affected the reference for the TOE?
* Has it affected the list of configuration items for the TOE?
* Has it affected any of the TSF abstraction levels, that is, the functional specification, the TOE design, or the implementation representation?
* Has it affected the architectural description (if the assurance baseline includes a component from the ADV\_ARC family)?
* Has it affected the mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design (if the assurance baseline contains a component from the ADV\_TDS family), and to the implementation representation (if the assurance baseline contains a component from the ADV\_IMP family)?
* Has it affected the guidance documentation (if the assurance baseline includes a component from the AGD class)?

* Has it affected the testing documentation, that is, the analysis of test coverage, the analysis of the depth of testing or the test documentation (if the assurance baseline includes a component from the ATE class)?
* Has it affected the vulnerability analysis?

## Impact of the changes on the Security Target

To help evaluate the impact on the changes of the Security Target, first, here is an extract of some of the Security Functional Requirements (SFR) in the PP [2].

| **SFR** | **Requirements** |
| --- | --- |
| FDP\_ACF.1.1 | The TSF shall enforce the access control to objects based on security attributes. |
| FDP\_ACF.1.2 | The TSF shall enforce rules to determine if an operation among controlled subjects and controlled objects is allowed. |
| FDP\_ACF.1.3 | The TSF shall explicitly authorise access of subjects to objects based on additional rules. |
| FDP\_ACF.1.4 | The TSF shall explicitly deny access of subjects to objects based on the rules. |
| FDP\_IFF.4.1 | The TSF shall enforce the information flow control to limit the capacity of illicit information flows to a maximum capacity. |
| FDP\_IFF.4.2 | The TSF shall prevent the following types of illicit information flow : tcp shell or http shell. |
| PMM\_IF.1.1 | The TOE shall maintain an outgoing heart-beat data flow with other platooning vehicles as specified below: From TOE to VCS (and then to another vehicle TOE). Messages transmitted shall contain the following data computed from the TOE vehicle sensors/algorithms: Vehicle unique identifier - Vehicle speed - Direction - Geo-Position - Timestamp. |
| PMM\_IF.3.1 | The TOE shall maintain an incoming flow with other vehicles informing the TOE vehicle about emergency brake maneuvers as specified below: From (another vehicle TOE to vehicle) VCS to TOE. Messages transmitted shall contain the following data: Unique identifier of the vehicle to which the emergency brake has been issued - Emergency brake identifier - Timestamp - Digitally signed certificates. |

Table 2: Extract of Security Functional Requirements (SFRs)

Start by identifying the related Item of the ToE :

* *SafeSecPMM*
* *iptables*
* *netFilter*

This will allow to eliminate the SFR not related to our firewall update.

| **Tag** | **related Item** |
| --- | --- |
| PMM\_IF.1.1 | SafeSecPMM |
| PMM\_IF.3.1 |  |
| FDP\_ACF.1.1 |  |
| FDP\_ACF.1.3 |  |
| FDP\_ACF.1.4 |  |
| FDP\_IFF.4.1 |  |
| FDP\_IFF.4.2 |  |
| FDP\_ACF.1.2 |  |

Table 3: Requirements per component of the TOE

Then link the issue to the SFR, define if there’s a security impact and justify your choice :

| **Issue** | **Tag** | **Requirements** | **Impact** | **Justification** |
| --- | --- | --- | --- | --- |
| [2](https://github.com/cetic/sparta/issues/2) | FDP\_ACF.1.2 | The TSF shall enforce rules to determine if an operation among controlled subjects and controlled objects is allowed. | False | The changes to the code of ipTables do not affect security requirements as it concerns only display. |
| [3](https://github.com/cetic/sparta/issues/3) | FDP\_ACF.1.2 | The TSF shall enforce rules to determine if an operation among controlled subjects and controlled objects is allowed. |  |  |
| [4](https://github.com/cetic/sparta/issues/4) | FDP\_ACF.1.3 | The TSF shall explicitly authorise access of subjects to objects based on additional rules. |  |  |
| [4](https://github.com/cetic/sparta/issues/) | FDP\_ACF.1.4 | The TSF shall explicitly deny access of subjects to objects based on the rules. |  |  |
| [4](https://github.com/cetic/sparta/issues/4) | FDP\_IFF.4.1 | The TSF shall enforce the information flow control to limit the capacity of illicit information flows to a maximum capacity. |  |  |
| [4](https://github.com/cetic/sparta/issues/4) | FDP\_IFF.4.2 | The TSF shall prevent the following types of illicit information flow : tcp shell or http shell. |  |  |
| [5](https://github.com/cetic/sparta/issues/5) |  |  |  |  |
| [5](https://github.com/cetic/sparta/issues/5) |  |  |  |  |
| [5](https://github.com/cetic/sparta/issues/5) |  |  |  |  |
| [5](https://github.com/cetic/sparta/issues/5) |  |  |  |  |
| [2](https://github.com/cetic/sparta/issues/2) |  |  |  |  |
| [3](https://github.com/cetic/sparta/issues/3) |  |  |  |  |

Table 4: Impacted requirements

1. reference image: <https://xerocrypt.wordpress.com/2013/08/26/what-exactly-are-netfilter-and-iptables/> [↑](#footnote-ref-1)
2. Firewall rules are not updated [↑](#footnote-ref-2)
3. <https://www.netfilter.org/projects/iptables/files/changes-iptables-1.8.7.txt> [↑](#footnote-ref-3)