TRUSTONIC riscure

Security certification considerations when choosing a secure product

Understanding Common Criteria and Evaluation Assurance Levels, and putting these into context when choosing secure products and services

Contents

Executive summary

The modern vehicle is not just a car: it is a complex, connected, computer ecosystem. As such, the automotive industry faces all the cybersecurity issues inherent within the wider software sector. So how do you choose a secure, future-proof platform that will protect your vehicle and your customers from real-world threats throughout the lifetime of the vehicle?

This paper discusses the role that security certification plays when choosing a secure solution that will benefit your customers now, and that will provide a future-proof platform for the emerging automotive cybersecurity threat landscape, and address legislation such as UNECE WP.29.

In this white paper the automotive industry is used as an example. However, the approaches and recommendations contained within this paper can be applied equally to other vertical markets and product types.

This paper provides value to:

- OEMs seeking to secure the modern, connected vehicle or set a secure foundation for future revenue streams such as the monetization of vehicle data

- Executives such as CEOs, CTOs and CFOs who want to prepare their cybersecurity strategy and understand the importance of designing security in from inception to meet current and future legislative requirements

- Product managers, especially those involved in vehicle connectivity - whether traditional telematics units, ADAS systems, or autonomous driving technology

- Security, quality and development teams seeking to understand security certification, particularly in the context of the wider security solution

- Business development and digital revenue teams wanting to understand the importance of building a robust, secure platform, especially for next-generation capabilities

- Procurement teams who want to develop a greater understanding of the risks associated with their buying decisions

This is the second in a series of papers on the role and value of security testing, evaluation and certification in the design, development and launch of secure products and services. In this paper, we focus on understanding Common Criteria (CC) for Information Technology Security Evaluation certification and the different levels and components associated with a CC evaluation. We will use the example of the TEE (Trusted Execution Environment) to show how security certification should be considered in the wider context of choosing an overall solution. Although there are other security certifications relevant to vehicles - such as those associated with payment technologies - the general principles and recommendations are the same.

Trustonic's mission is to embed the best security into the world’s smart devices and apps; empowering vehicle, mobile and IoT developers to build in the trust required to deliver simple, fast and secure solutions.

Riscure is a leading vendor of security services, tools and training for edge devices. Our tooling helps global technology leaders to build robust hardware and software solutions. Riscure security analysts bring top-notch security expertise to development teams and aim to run no-pain certification projects. Built on a wealth of security research and extensive practical experience, Riscure is well recognized for its technical leadership.

Trustonic and Riscure work closely together to drive more secure technology implementations. The two companies share a vision to help the ecosystem to better secure devices, apps and data. This paper represents a joint effort to provide additional clarity for readers seeking to understand the security certification processes with a focus on the critical connection between Evaluation Assurance Level (EAL) levels and the potential evaluation scope.

[1] Whitepaper – Demystifying Security Testing, Evaluation & Certification for Devices & Apps

Introduction

The digitization of in-car systems is the foundation on which the next wave of innovation in the automotive industry is built, whether it is connected cars, electric vehicles, autonomous driving or shared mobility. However, with increased digitization comes the increased risk of cyberattack[2] . If a car's security is compromised, this can result in the theft of personal data or the car itself, a risk to the vehicle's security and safety mechanisms or, in extreme cases, full remote control of the car. And, with the dawn of autonomous vehicles, these risks are only set to increase due to the dependency on software communication channels. Failure to protect against these risks could have a catastrophic effect on consumer confidence, privacy, brand reputation and worse, vehicle occupant and pedestrian safety.

The "hack" in 2012 of a Toyota Prius and Ford Escape by security experts Dr. Charlie Miller and Chris Valasek is one of the more dramatic examples. They showed how they were able to attack a 2010 Ford Escape and 2010 Toyota Prius by cutting the power steering, taking control of the horn, and spoofing the GPS, as well as the dashboard displays. Miller and Valasek then went on to demonstrate how they could remotely hack a Jeep Cherokee via its internet connection, effectively paralysing it.

To perform these hacks, they exploited the automated features in these vehicles. They used the Prius' collision avoidance system to slam on its brakes, the Jeep's cruise control system to make it accelerate, and the Jeep's parking assistance to turn the steering wheel, even when it was moving at 80 miles/hour.

These flaws are serious enough in vehicles with a few automated features. However, in a driverless level-5 autonomous vehicle, the computer has complete control and there is no manual override. Miller states that solving autonomous vehicles' security weaknesses will require a serious rethink of their architecture.

[2] Upstream Security report "Upstream Security's 2020 Global Automotive Cybersecurity Report" cyber-attacks against vehicles have increased by 99% between 2018 and 2019.

In addition to protecting vehicles from thieves and cyber criminals, there is also the need for manufacturers to build a secure platform for future revenue growth, one that customers can trust. This secure platform must also meet minimum regulatory requirements which affect not only vehicle development and production but also post-production activities, including the ability to fix security issues years after the sale of the vehicle.

The challenge is therefore one of choosing a robust, future-proof security solution that meets all these requirements. And, part of this challenge, is understanding the various security certifications relevant to the different use cases in the automotive industry, and the importance of the certification levels in the context of the complete solution.

The robustness of a security solution for current and future threats depends on several factors such as:

- Does the attack model resemble real attacks present in the wild?
- Have all possible paths toward security compromise been considered? Will the paths include all components of the complete product?
- Has the security assessment been performed with a high enough Vulnerability Analysis (VA) level to capture the defined attacks in the wild and future attacks, with sufficient depth?

The assurance level of the security of a product is a concept defined in Common Criteria as a measure of confidence that the product or component meets the security functional requirements.

In addition, the assurance level provides a measure of the depth to which the assessment is performed. The assurance may cover the robustness of a certain level for VA, additionally verifying the secure development process and potentially using formal methods to provide proof.

In this paper, we focus on Common Criteria security certification, and we consider this in the context of evaluating a Trusted Execution Environment (TEE). Although there are other security certifications that could be applicable to the automotive industry – such as FIPS and PCI DSS, in the case where the vehicle is the transacting entity such as payment for apps or tolls – we will show that the general principles are the same.

Understanding Common Criteria and EAL

Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria, or simply as CC) is an international standard (ISO/IEC 15408) for the security evaluation and certification of information technology (IT) products.

CC provides a structured framework that is generic, so it can be applied to any IT product. The CC framework provides the IT community with a common language and metrics to address IT security.

Three entities are involved in a CC evaluation:

- The vendor which provides the product, defines the Target of Evaluation (TOE) which is the portion of the product that will be evaluated, and the Security Target (ST). These are explained in more detail below
- The Security lab, such as Riscure, who performs the evaluation and presents the results to the Certification Body
- A Certification Body who monitors, supervises, and approves the lab activities and issues the certification for the TOE[3].

CC certificate recognition depends on the country issuing the certificate, the EAL (Evaluation Assurance Level) of the certificate, the type of product being certified, and if the product claims conformance to a recognized Protection Profile or not (see below).

[3] Certification Bodies for Common Criteria are typically national government agencies such as the BSI in Germany, ANSSI in France and the NSCIB in The Netherlands.

Protection Profiles and Security Targets

There are two important documents in CC evaluations:

1. The Protection Profile (PP) – defines the security requirements of consumer groups and communities of interest for a product type; in other words, these are the minimum set of requirements your product must fulfil. PPs are generic for a product type, as opposed to a Security Target that is written for a unique TOE. PPs are certified by a CC scheme, such as PP for vehicle-to-everything (V2X) certification or PP for TEE certification. Some markets demand that your product type complies to a specific PP. The PP document includes the following key sections:

a. “Security Problem Definition” that describes the assumptions, organizational security policies and type of threats the product claims to protect against. For example, in the case of the TEE, this includes software attacks, non-invasive physical attacks, remote attacks etc.

b. “Security Objectives”; for example, for the TEE this includes secure boot (O.INITIALIZATION), application isolation (O.TA_ISOLATION), key management (O.KEYS_USAGE), among others.

c. “Security Requirements” where the minimum set of assurance requirements and functional requirements are defined.

2. The Security Target (ST) – defines the security requirements of a specific TOE[4] in other words, this is the scope of the evaluation for a particular TOE. The ST is mandatory and defines the exact threat model that the product claims resistance to, and the Evaluation Assurance Level (EAL). An ST may comply with one or several PPs, meeting all the requirements defined in the PPs, and it can add and/or increase evaluation items beyond the minimum requirements defined in the PP.

Importantly, an ST can be a free - format ST which does not claim conformance to a PP; in this case the scope is determined by the vendor themselves. This suggests you can only increase the level of assurance in the ST, where in fact the opposite is true. When a vendor writes a Security Target to support a product certification, there are options: (i) to comply with an existing Protection Profile, or (ii) to create a fully customized ST. Security Targets can also adhere closely to an existing PP; this is not formally recognized, but it can be mentioned in the ST. The process of tailoring an ST is explained in more detail below.

[4] The TOE should consist of the following: the specific product version and corresponding guidance documents

EAL levels

Common Criteria Evaluation Assurance Level (EAL)	Description
EAL 1	Functionally tested
EAL 2	Structurally tested
EAL 3	Metholodically tested and checked
EAL 4	Metholodically designed, tested and reviewed
EAL 5	Semi-formally designed and tested
EAL 6	Semi-formally verified, designed and tested
EAL 7	Functionally designed and tested

The CC evaluation methodology is divided into seven Evaluation Assurance Levels (EALs) with EAL1 being the lowest and EAL7 the highest level. Each level must satisfy a predefined minimum package of assurance components requirements, as summarized in the following table:

Note that there are regional differences between CC schemes; for example, between Europe, Asia and the US. Common Criteria Recognition Agreements (CCRAs) also exist between countries. For more information about these, see https://www.commoncriteriaportal.org/.

Assurance components and the attack potential (AVA_VAN)

Each EAL has a predefined package of assurance components associated with it. The predefined EALs can be extended by “augmenting” with additional or higher level assurance components; for example, an EAL5+ can be achieved by increasing the level of one or more assurance components normally associated with a higher level, or by adding a component that is not part of EAL5 package; for example, ALC_FLR.1, which is about the Flaw Remediation process. See Appendix 1 for a list of assurance components by EAL.

Another example is the AVA_VAN component, which defines the level of rigor applied in the vulnerability analysis and the attack resistance that the product needs to achieve regarding the threat model.

There are five levels for AVA_VAN:

Vulnerability Analysis (AVA_VAN)	Description
AVA_VAN.1	Vulnerability survey and resistance against a basic attack potential
AVA_VAN.2	Vulnerability analysis and resistance against a basic attack potential
AVA_VAN.3	Focused vulnerability analysis and resistance against an enhanced-basic attack potential
AVA_VAN.4	Methodical vulnerability analysis and resistance against a moderate attack potential
AVA_VAN.5	Advanced methodical vulnerability analysis and resistance against a high attack potential

When a TOE passes an AVA_VAN.x level, this means the target scope has proved resistance to an attacker with a certain attack potential (based on the availability of specialist tools, time or knowledge as well as a few other parameters). For example, if we take the Smart card industry, the minimum assurance level is EAL4 augmented with assurance classes aimed at proving the product is sufficiently resistant against a high attack potential.

Putting EAL into context

As we have seen, there are several EALs, each characterised by a predefined package of assurance components. CC evaluation involves assessing whether the desired assurance level is achieved or not by, among other activities, appraising aspects such as the product functionality, the quality of the developer test campaign, the documentation requirements for design and implementation, as well as the site security and other relevant aspects. All these aspects build assurance into the product. Different levels of vulnerability analysis are also conducted, ranging from a basic analysis to an advanced methodical vulnerability analysis.

CC methodology is flexible, allowing vendors to choose the level of certification they want to achieve and to tailor the assurance requirements and evaluation efforts, in cases where the evaluation is not conducted against the approved PP.

This approach covers a wide variety of use-cases; however, due to complexity, it is possible that the target use-cases and certification results are misunderstood by the consumer of the certificate.

Undertaking a CC evaluation can be a time-consuming and costly process, particularly for the higher EALs. Typically, a CC evaluation takes around 3 months (for EAL2-3) and 6 months to a year for a smartcard with high assurance (EAL6-7), depending on the quality and completeness of the TOE. As a result, vendors will seek to find the best ratio between cost, evaluation level and evaluation scope. Sometimes this means reducing the scope of the security evaluation to achieve the certification and to keep costs down or to manage the wider system level complexity.

“Vendors will seek to find the best ratio between cost, evaluation level and evaluation scope”

As a result, the EAL cannot be viewed in isolation from the Security Target (ST) document which defines the security properties, assessment scope and threat model. For example, a standard EAL4-certified secure element (smartcard technology) used to protect the storage of a cryptographic key often has a higher security level than a complete TEE OS fully certified with a higher EAL, including EAL7+. This is because smart card technology, and its certification process, answers to a threat model which includes some advanced and destructive hardware attacks.

The different CC levels are a measure of the level of assurance that claims about the security of a product have been rigorously tested and independently verified.

By design, CC levels (EAL6 to EAL7) are not a measure of the robustness of the product in the vulnerability assessment sense (AVA_VAN5). Instead, the aim of these levels is to offer greater assurance from additional requirements on the rigor of the modelling and verification approach in the development process; for example, by mandating the use of semi-formal and formal specification and verification techniques. Increasing the assurance level has an important role for a security guarantee in the market.

Taking a holistic approach to security evaluation

The security of an end-user ready product should always be assessed in its entirety and not simply at the security certification level of its individual components. This is because attackers will always target the weakest point in a solution and are typically highly skilled at identifying such weak points, as shown in the Miller/Valasek example above.

To illustrate this, we will consider the role of the Trusted Execution Environment (TEE) in securing sensitive data and protecting security-critical code. We have chosen this example because Trustonic believes the TEE will play a key role in ensuring that vehicles, and the devices that they interact with, are fully protected.

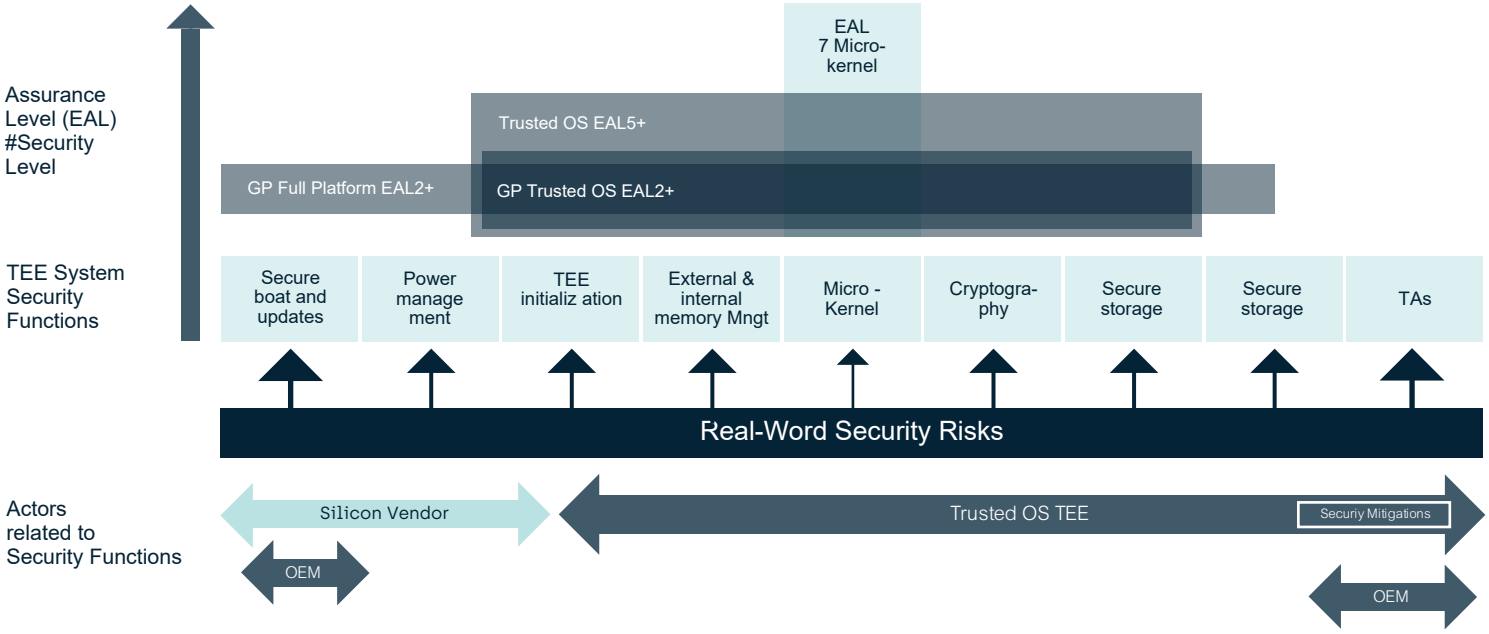
“Attackers will always target the weakest point in a solution”

The TEE is a secure operating system (OS) that runs alongside the main device OS environment such as Android or QNX (sometimes called the REE – Rich Execution Environment). The TEE isolates critical code and data in a safe, hardware-isolated world, protecting it from attackers. Due to its small size and isolation from the rest of the system, the TEE minimizes the attack surface, preventing threats such as reverse-engineering, tampering, malware, and Trojans.

The TEE consists of several components that work together to provide a complete system, including cryptography and secure storage, together with components that support these critical security functions such as device drivers, the kernel and other software components. Evaluating one of these components independently would provide partial security assurance.

The following diagram shows the main TEE Security Functions, real-world security threats, and EALs. For the purposes of illustration, we feature a TEE with components certified with different scopes and to different levels. The diagram shows that the kernel is the least exposed component, and that threats tend to affect the other components, particularly drivers and Trusted Applications (TAs).

As we have seen, TEE product vendors can restrict the scope of what is evaluated in a CC evaluation, sometimes to only the one component. However, a TEE OS is a complete system that provides cryptography APIs, secure storage, and secure application management. All the components involved in the enforcement of these security functions are critical for total protection.



As the diagram above shows, having one component certified in isolation against a high EAL level, must be supported by evaluating other components in the system responsible for the overall security robustness of the final product. The wider components in an open TEE OS may include drivers and Trusted Applications built by third-party developers and, if these components are not developed to the same quality as the certified component, this can lead to potential security vulnerabilities arising in the code base. Even worse, it could lead to the final product user (the vehicle OEMs) not understanding the overall resilience of the integrated solution against external attackers.

Consequently, another important point to consider is the list of hardening features that the TEE OS and its SDK offer to protect the driver and TA drivers from active attacks. As highlighted in Riscure's recent whitepaper "Security Pitfalls in TEE Development", Trusted Applications and drivers suffer from many of the same security weaknesses as Rich Operating System applications - everything from memory corruptions to program logic-related issues.

Memory corruption vulnerabilities continue to be one of the most prevalent problems in the TEE ecosystem, with such issues present in production code, and the security impact ranging from the exposure of data to run time control of the target.

For this reason, Riscure recommends you:

“introduce software exploitation countermeasures for additional security. Some examples of software exploitation countermeasures include Address Space Layout Randomization (ASLR), stack canaries, control-flow integrity, non-executable stack and heap (NX), guard pages and so on”

Therefore, when evaluating the security of a solution such as a TEE, it is important that the scope of the evaluation encompasses the entire solution or that there is a follow up evaluation of the other components, since an attacker is presented with a complete solution. When CC evaluation is well scoped and conducted, the “attacker” and the “evaluator” become one.

Failure to adequately protect the entire TEE OS with all its security functions in a vehicle could result in attacks such as:

- Extraction of the car’s GPS history (a privacy issue). For example, USA Today discovered that vehicle-hire companies routinely fail to delete personally identifiable information that renters have input into a rental car’s infotainment system.

- Ransomware in the TEE, leveraging the Trusted User Interface (TUI) to block the screen. If malware infects the TEE, there’s a possibility that a cybercriminal will have enough privileges to launch an attack.

- Extraction of digital car keys leading to the theft of the vehicle. For example, tests by the ADAC — the German automobile association — showed that vehicles from almost 30 manufacturers could be unlocked using a relay amplifier and transmitter to ‘trick’ a vehicle into thinking its key fob is nearby. Using this method, the transmitter effectively becomes the key, enabling thieves to unlock the car, start the ignition and drive away in under 60 seconds.

Therefore, when determining the security robustness of a product, use the minimum common EAL level for all the components that are storing or processing the assets relevant for the final user (in this case OEMs). Do not suppose that the EAL level of the overall product is based on the highest-rated individual component as this will lead to inaccurate assumptions being made about the overall security of the system. This is explained in more detail in the next section.

Leveraging the GP TEE Protection Profile

One of the main advantages of using a recognized Protection Profile as reference for certification is that it allows you to easily compare two products, because the scope is clearly defined and remains constant. Without this, it is difficult to compare products due to different evaluation scopes.

A protection profile sets a minimum assurance level that a product needs to fulfil for different assurance classes. It is possible to increase the assurance level for a product by increasing assurance of some or all classes, and a higher assurance level of an existing Protection Profile should cover the whole scope of the Protection Profile.

For example, to evaluate the security of a TEE as an integrated system, a typical approach would be to evaluate against the GlobalPlatform TEE Protection Profile. Think of this as a “TEE recipe” in which all the security requirements expected from such a product are listed. To complete certification under this PP, all the TEE components are evaluated, giving a more complete sense of the achieved system security.

This approach considers software and hardware attacks against the TEE with an “enhanced-basic” attack potential (EAL2+ augmented with AVA_TEE.2). This approach is centred on reviews of the implementation together with additional assurance elements such as fuzzing of TEE interfaces.

It is also possible to add use-case specific security services such as data rollback protection using Protection Profile modules, but these are focused on specific use cases where protected data is considered an asset. GlobalPlatform (GP) aims at providing statements on the general robustness of the TEE as a support platform for specific use cases. GP evaluation considers generic attacks on unknown assets managed by the TAs using the TEE. From a process perspective, GP acts as a certification body.

Conclusion

When choosing a security product, security certification often plays a key role in product selection. A higher EAL provides the market (in our automotive example, the Tier 1 or OEM) with a specific higher level of assurance regarding claims about the security of the specific part or complete product, which has been rigorously tested and independently verified. However, a higher EAL with a limited scope is not easily translated into a measure of the robustness of the overall product, unless all product parts are independently verified to the same EAL as well as the integrated product.

Certification should always be considered in the wider context of the security required from the entire solution and what it is that you are seeking to protect. For example, in the case of the TEE and CC certification, the EAL of an individual component in isolation offers limited information about the security of the complete TEE system. Its use is compromised if other components do not follow the certification level and user guidance documents.

In cases where vendors define the scope of what is evaluated (i.e. they do not follow an approved Protection Profile in the Security Target), it is important to understand exactly what was assessed and what was not. There is a difference between a product (the solution used by a user or a device) and the Target of Evaluation (which may be a full product or just a component). A recognized Protection Profile is useful in this respect because it enables you to compare two products, like for like. Therefore, it is recommended that a detailed review of the scope of the assessment is conducted (by reviewing the contents of the Security Target associated with the specific certificate), when seeking to understand the applicable level of protection a solution can provide.

In conclusion, therefore, it is critical that the Security Target scope addresses all the security relevant components of the final solution and the applicable list of threats that the product is designed to mitigate. When properly scoped and with all the components and integration evaluated, the security evaluator will act in the same way that an external attacker acts, thus providing more assurance to users of the final product regarding the achieved security robustness of the product.

Appendix 1 - Assurance Components by EAL

Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life-cycle support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

References

- https://www.trustonic.com/news/technology/secure-developent-lifecycle-mobile-app-security-testing-certification/
- https://www.upstream.auto/upstream-security-global-automotive-cybersecurity-report-2020/
- https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/cybersecurity-in-automotive-mastering-the-challenge#
- https://csrc.nist.gov/publications/detail/fips/140/2/final
- https://www.pcisecuritystandards.org/pci_security/
- https://www.commoncriteriaportal.org/
- https://www.trustonic.com/news/blog/the-changing-face-of-automotive-cyber-attacks/
- https://globalplatform.org/specs-library/tee-system-architecture-v1-2/
- https://www.riscure.com/publication/security-pitfalls-in-tee-development/
- https://threatpost.com/modern-car-warning/142190/
- https://www.bbc.co.uk/news/business-49273028
- https://globalplatform.org/specs-library/tee-protection-profile-v1-2-1/
- https://globalplatform.org/resource-publication/an-exploration-of-tee/
- https://www.commoncriteriaportal.org/files/ppfiles/anssi-profil_PP-2014_01.pdf
- https://www.sae.org/binaries/content/assets/cm/content/topics/cybersecurity/securing_the_modern_vehicle.pdf
- https://www.upstream.auto/research/automotive-cybersecurity/

Glossary

Term	Description
ADAS	Advanced Driver-Assistance Systems
AVA_VAN	Vulnerability Analysis component
CC	Common Criteria
CCRA	Common Criteria Recognition Agreement
EAL	Evaluation Assurance Level
GP	GlobalPlatform
OEMs	Original Equipment Manufacturers
OS	Operating System
PP	Protection Profile
REE	Rich Execution Environment; for example, the Android OS
ST	Security Target
TA	Trusted Application
TEE	Trusted Execution Environment
TOE	Target of Evaluation
V2X	Vehicle-to-Everything

Authors

- Mafalda Monteiro Oliveira Cortez, PhD, Certification Team Lead, Riscure
- Jasmina Omic PhD, Product Manager Services, Riscure
- Baptiste Gourdin, Security Architect, Trustonic
- Andrew Till, Automotive Specialist, Trustonic
- Amanda Lindsay, Technical Author, Trustonic
- Nikola Medic, International Sales and Business Development Manager, Riscure
- Christophe Colas, SVP Licensing and Corporate Projects, Trustonic

riscure

Challenge your security

TRUSTONIC