Text Proposal for: Sections 8. and/or E.6 Security of IEEE 802.1DG/D1.3

Max Turner
Ethernovia
Feb. 2021

Glossary

Definition Security vs. Safety

While security here is to describe a malicious and deliberate manipulation of software, configuration or communication data, safety (as e.g. per ISO 26262) is usually concerned with random (non deliberate) or accidental changes in software, configuration or communication data.

This document will use safety in the sense of ISO 26262 as well as in the sense of anything that may bodily harm the inhabitants. This would be any loss of control of the vehicle or harmful actions by any vehicle system.

Security is used when deliberate changes to the vehicles software, configuration, or communication data aiming to circumvent limitations imposed by the current user, owner or manufacturer are to be prevented. Examples may be activation of features which are not paid for, using a rental/shared car without payment, or gaining access to steal items from the interior.

Obviously the two intersect where deliberate interference intentionally or unintentionally leads to bodily harm. One could therefore argue, there is no Safety without Security, but there may well be a certain level of Security without Safety.

From an implementation perspective cryptographic functionality used for security is usually difficult to validate against the requirements of safety due to their complexity. This often leads to separate implementations.

Definition Authentication

Authentication allows to identify an entity or person and verify a message has actually been sent by this entity.

Definition Authorisation

An entity or person may be entitled to execute a certain functionality, the entity is the authorized to execute a certain action.

Definition Integrity

Integrity of data means it is unaltered from the original. This is often viewed as the intersection of safety and security, as both of them aim to achieve this.

Definition Encryption

If a message can not be read/understood by an entity that is not authenticated to do so, then this message is called encrypted. It is important to note, that a message may well be proven unmodified (integer) and the sender authenticated, but not encrypted. On the other hand a message may be proven unmodified (integer) and encrypted, but the sender may not necessarily be authenticated.

Use-Cases

Semiconductor Manufacturing

Semiconductor components (ICs) must be able to fit into ECUs of different Tier 1s and OEMs. Therefore theft or copy of an IC shall not easily enable falsifying ECUs.

ECU Manufacturing

ECU hardware is mostly produced in assembly lines outside the OEMs vehicle assembly plants by Tier 1s. Security risks including hardware and key material theft or software manipulation must be taken into account.

ECUs falsely diagnosed as defective and/or stolen form a Tier 1 may be later sold as spare parts and, depending on the configuration, enable features the customer did not pay for.

Vehicle Manufacturing

A large vehicle manufacturer builds about 1 vehicle per minute per assembly line in multiple plants around the world. This makes it crucial for the process to be fully automated. There can be no manual intervention before the assembly of a part (“personalizing” to a vehicle) or during the assembly (manual confirmation or code entry). The installation of key material, credentials or certificates, the network configuration and the start-up of secure communication must be fully automated inside the vehicle as well as all aspects concerning plant infrastructure (e.g. PKI). This automation must be performant (takt times between assembly steps are measured in units of seconds) and must potentially cope with the loss of power as the vehicle moves along the assembly line.

A highly distributed approach to infrastructure components is considered good practice as a loss of connectivity to same infrastructure should not lead to a stop of the assembly line as this would incur high cost. Unfortunately placing infrastructure directly at the assembly line may need additional layers of security as the manufacturing environment is never fully secure. This is particularly true if third party manufacturing lines are used.

The principle of fail-secure may lead to interruptions of the assembly process if a vehicle can not be moved away from the assembly line as planned.

Automotive ECU connectors are carefully cost engineered to withstand a certain number of connection cycles and the least possible of those should be used up before delivery to the first customer as they are mainly intended for repair work to be executed over the lifetime of the product.

Partial operation of network segments may be desirable to check for missing or malfunctioning components early in the assembly process where access is still possible without significant dis-assembly.

Vehicle Start-Up

Many features of a vehicle must be available within just a few seconds after start-up (e.g. FMVSS111 – rear view camera). Particularly for ICE vehicles this means a cold boot-up from a very low energy state within a very short time. Allowing for sufficient entropy to potentially generate 100s of sessions keys can be non-trivial.

Vehicle start-up can not depend on vehicle external infrastructure as cellular networks, WiFi connectivity or GNSS reception are not available in all locations like underground paring. A fail-secure lockout of the legal customer can quickly lead to high cost if the car must be towed.

While this document only concerns itself with the networking infrastructure one needs to account for the time taken by CPUs to execute secure boot.

(Session-)Key generation and potential exchange (for symmetric keys) will likely have to happen in parallel within non-connected islands of the network and should allow bi-directional initiation (e.g. for IPsec) as to not have one component wait because of the delay in another.

Vehicle Operation

Operation of a vehicle is no longer limited to driving from A to B. The customer may spend time inside a parked car e.g. sleeping and/or listening to music or watching a video. The customer may use an online service to check on the status of the car (windows and doors locked?, state of charge for EV, fuel tank level for ICE). A parked EV may be charging or waiting for an economic (lowest cost of energy) time to charge. An EV not currently charging (or even while charging), but specifically a parked ICE vehicle want to minimize the consumed power for physical intrusion detection and surveillance systems to a minimum. This is due to the energy reserve needed to start to ICE as well as to the charging efficiency of the EV and the difference in conversion efficiency between high and low voltage systems. A very special case of operation is the diagnostic and testing mode of the vehicle.

If vehicle security depends on infrastructure, it is important to allow for graceful aging of these infrastructure systems over the 15 to 20 year operational life-time of the vehicle.

Due to the power restrictions when parked, which are mentioned throughout this document, specifically for ICE vehicles, but to a different degree also for EVs, a vehicle may have at start-up a very distorted view on the actual date and time of day (as defined by TIA). With an operational lifetime of 15 to 10 years or more this may lead to challenges in validating certificates, which may expire.

ECU Theft

Stealing a whole vehicle is no longer the main objective of criminal activity. The re-sale of spare parts like air-bags and infotainment systems (head-unit) is much more prevalent attack.

Vehicle repair

Neither the customer nor a repair shop can reliably be trusted to execute only legitimate operations on a vehicle once it is sold. Activation of un-paid features (e.g. engine “chip tuning”) or modification of functionality (e.g. operating convertible roof at unsafe speeds) have long been an issue causing warranty cost if the modification goes undetected.

Threats and Attack Vectors

Modification or insertion of messages into the in-car network

This requires physical access to the vehicle. The most likely attacker here are malicious repair shops or DIY activists who want to manipulate the feature set of the vehicle or even gain access to the OEM backend server via the vehicle.

Reading of messages in the in-car network

This requires physical access to the vehicle. The most likely attacker here are malicious repair shops or DIY activists. While most analysis are concerned with the data contained within these messages, it seems at least equally important to point out, that these messages can be collected off-board (e.g. via a cellular modem) for a long time. If done on multiple vehicles this allows analysis of the security implementations used. Such a long term sniffing may then enable the attacker to modify or insert messages at a later time, in case configurations in different vehicles reveal details of the used cryptographic methods and keys if compared with each other.

Insertion of messages via the OBD-port

It has been argued in the past, that the OBD-port is only accessible for someone who has access to teh vehicle interior. With BlueTooth or cellular adapters attached in order to augment non-integrated navigation systems, company fleet management or for insurance purposes this is no longer true.

Insertion of messages via vehicle internal WiFi-AP

A vehicle may include a WiFi access point in order to make internal information or even control available to a mobile device. As the ECU implementing the WiFi-AP also has connectivity to other systems inside the vehicle this offers a path for an attacker.

The basic assumption here is that a mobile device is connected via WiFi (or BlueTooth or similar) to the vehicle. On the mobile device is an application which should allow the user to change for example the entertainment volume or the ambient temperature or the seat position. While all of this sounds like rather low security profile use-case, it can quickly turn into a safety issue, if the driver's seat is being moved in a way the driver may loose control over the vehicle or where the diver is startled by a very loud sound being played out.

If a mobile device has control over some vehicle internal systems there is at least two elements where such a control path can break out and malicious control over other systems. The first being the access point where the wireless signal is received and somehow translated onto a command for anther vehicle internal system which actually executes the requested functionality and represents the second point of attack.

Furthermore the mobile device is likely connected to the internet and therefore needs to itself be secured against remote control of the app which, if operated by the user, is permitted to execute control over selected vehicle functions.

Insertion of messages via a cellular interface or vehicle internal WiFi-STA (internet)

Some vehicles can connect to an external WiFi access point, e.g. in order to download OTA data in areas where cellular coverage is insufficient. This potentially exposes the ECU implementing the WiFi-STA to attacks from the internet and as this ECU also has connectivity to other systems inside the vehicle this offers a path for an attacker.

Insertion of messages to/from the smart-charge port

As charging ports are often placed in public spaces, they can be manipulated by an attacker. This can be as simple as inserting an adapter into the connector. The goal of the attack can be the vehicle (e.g. to open doors) or the charging infrastructure (e.g. to not pay for charging).

Modification or insertion of messages into the backend link

Spoofing the backend link

Specifically for OTA functionality it is important to ensure the vehicle connects to the actual OEM backend and not to a manipulated or spoofed server. This is particularly difficult for vehicles which do not have constant connectivity. The longer the interruption of connectivity is, the harder it will be for the vehicle to ensure the apparent backend is actually authentic. One element of this problem is the lack of accurate time in a vehicle when it is not operated for ICE vehicles and to a different degree for EVs when they are not being charged.

Modification of Software (code or configuration) in RAM

Modification of Software (code or configuration) in NVM

In order to make a malicious change persistent over a power cycle, the NVM needs to changed. With modern ECUs using SSD like rather than Flash/EPROM like storage elements this may become easier and make secure boot and secure OTA more important.

Modification inside the OEM backend

If an attacker can gain access to the OEMs backend an OTA functionality can be misused to manipulate the vehicle's software and configuration. Without a sufficiently disjunct two-factor process, such attacks will be difficult to detect from inside the vehicle.

Possible solutions

Autosar SecOC or TLS

AR SecOC provides application to application security. This means start-ups need to be secured for every TCP/TLS or UDP connection. For n ECUs this may lead to n^3 connection start ups to be performed.

IPsec

IPsec provides ISO/OSI Layer 3 connection security. Meaning multiple applications residing on a single IP host share the secure connections established with other hosts in teh network. Still the establishment of IPsec connections within a network on n ECUs may lead to a start-up of n^2 connections.

IPsec is not bale to secure layer 2 protocols like IEEE17222 or IEEE802.1AS and has difficulties securing IP multicast data distribution or service discovery.

MACsec

MACsec only requires roughly n connections – or in this case links – to be started up for a network of n ECUs. MACsec can also protect at network level any protocol on that link.

On the downside, the use up MACsec on one link may very quickly require the use of MACsec on all links inside the vehicle, as one would not want untrusted information to gain “trust” by being forwarded from a non-MACsec link onto a MACsec enabled link.

SecureBoot

Behavioural analysis

Relation to the ISO/OSI stack

Safety/Security Layering