Student projects for CVII and Security

June 10. 2021

Background

- Fill in with info from Joby
- e.g. University, Professor, potential student information (course and study?)
- Time and duration of project

Context information for project proposals

These proposals are focused around a few existing standards:

VSS = Vehicle Signal Specification

A standard description format for data in automotive, and a set of standard data definitions for the automotive industry.

VISS (v2) = W3C-defined "web protocol" for accessing car data (which is described using VSS). This is a specification. There is at least one *complete* implementation (written in Go language) and some partial ones based on v1.

MQTT = Popular publish/subscribe protocol for data in IoT and automotive environments

Topic ideas

- Definition of access-control and authentication schemes
- Definition of practical PKI principles for an automotive environment
- Safe programming practices, including comparing languages and environments
- Evaluation of implementations for code quality / security vulnerabilities.

Project idea #1

Name: Define/implement authentication strategy for VISS protocol

Task summary: Define authentication scheme and encryption key management principles for VISS protocol and implement it

Introduction and context

VISS specification outlines a "role based" access control mechanism with several credentials deciding which signals shall be accessible. It defines the actors (e.g. client, access-grant-server, data-server), and some of the mandated technologies, such as Java Web Tokens (JWT) as the means of proving access to a certain resource (vehicle signal). However, it does not specify all details about how encryption keys are deployed on various actors, or exactly how the provided credentials shall be evaluated in order to determine access (the details of authentication and authorization)

Task specification:

Propose a solution for the parts that have been left open in VISS specification as described above, and implement them. Evaluate and report findings on the result.

Project idea #2

Name: Implement VSS access control for MQTT

Task summary: Decide how to describe access control groups for VSS signals and implement it in a MQTT environment.

Introduction and context:

VSS defines data items by means of attached metadata (signal type, data type, physical unit, description..).
It is possible to attach additional metadata using an additional "layer"

It is required (in basically all situations) to limit access to a selected set of data depending on who is accessing it. VSS defines all signals but does not group them into permission groups (it is user/context dependent). Therefore, it is required to im

Task specification:

1) Define a description format for signal permissions. (I.e. a group of signals that should be accessible under a certain permission name, and whether these are readable and/or writable).
This can be done as additional metadata in a "layer" for VSS or a similar approach.

2) Implement enforcement of the signal access control in an MQTT server

Alternative: Another data protocol / implementation might be substituted for MQTT, after discussion.

Project idea #3

Task name: Collect and document safe programming practices

Introduction and context:

For these technologies, the implementation is as important as the formal specification. Even with a "correct" strategy in theory, implementations can fail through typical programmer mistakes and bugs, often described as security vulnerabilities.

Methods to counteract:

- Diligent program design and knowledge about safe programming practices
- Manual code review
- Penetration testing, including fuzz-testing
- Tool-supported code review

Task specification:

- Collect and document safe programming practices
- Compare programming languages and other approaches regarding their support for safe practices
- Exemplify where these practices apply. Evaluate projects regarding if these practices are known and have been applied.

Project idea #4

Task name: Review existing implementations for security vulnerabilities

Introduction and context: (same as previous)

Task specification:

- Survey available code-scanning and similar tools for supporting security-focused code review
- Apply tools to existing projects and report findings