C Safety and Security Rules Study Group – progress report October 2018

Background

The strategy of the group has been to:

- take the existing TS17961 ‘C secure coding rules’ as the starting point for the security aspects
- consider incorporating MISRA C:2012 rules to address the safety aspects
- consider any other safety or security rules

The study group has been trying to categorise rules into three usage profiles:

- Safety only
- Security only
- Safety and Security

We have also been trying to identify:

- which rules should be diagnosed by static analysis tools, which may include compilers
- which are rules for programmers
- whether there is a need for a deviation process, along the lines proposed by MISRA
  .

Progress

So far we're just over half way through the MISRA-C rules.

After this is complete, the plan is move onto writing the new rules for the new technical document, addressing the three profiles mentioned above.

Some attempt has been made to begin writing - or 're-framing' - the rules so that they would be more suitable for static analysis tools when applied to large programs, but not much progress has been made here.

Overall progress is slower than hoped for, largely due to a mismatch between the precautionary approach wanted in the safety community (which typically is looking at small scale, new code development) and a desire to only be told about problems with demonstrable negative effects in the security community (tending to be looking at large systems including code and library reuse).

Challenges

We currently have no chairperson.

Recently there has been a lack of contributions from people with security-critical expertise, possibly due to constraints on availability more than any other factor.

If the final document is going to include a substantial part of MISRA’s IP, its not clear that the necessary permissions for us to republish it have been obtained

Reconciling the requirements of the safety and security communities