Contribution ID: **193** Type: **not specified**

New Smatch Developments

Wednesday, 22 September 2021 09:10 (25 minutes)

Smatch is one of the main static analysis tools used in the kernel. These days simple static analysis checks are increasingly implementing in the compilers. For Smatch the new work is in more complicated cross function analysis that compilers cannot handle.

This talk will give a brief introduction to the new Smatch Param/Key API which makes it easier to write advanced cross function checks and removes a lot of boilerplate code.

Then it will cover Smatch's "Sleeping in atomic" check. Checking for sleeping in atomic bugs requires complicated cross function analysis. This is an example of an advanced check with a lot of moving parts.

Finally, the talk will cover an in development check for race conditions. In some ways this is the most complicated Smatch check ever. Hopefully we can have a discussion about how to make this check better.

I agree to abide by the anti-harassment policy

I agree

Primary author: CARPENTER, Dan (Oracle)

Presenter: CARPENTER, Dan (Oracle)

Session Classification: Testing and Fuzzing MC

Track Classification: Testing and Fuzzing MC