Linux Plumbers Conference 2019

Contribution ID: **75**

Type: **not specified**

Formal verification made easy (and fast)!

Tuesday 10 September 2019 17:45 (45 minutes)

Linux is complex, and formal verification has been gaining more and more attention because independent "asserts" in the code can be ambiguous and not cover all the desired points. Formal models aim to avoid such problems of natural language, but the problem is that "formal modeling and verification" sound complex. Things have been changing.

What if I say it is possible to verify Linux behavior using a formal method?

- Yes! We already have some models; people have been talking about it, but they seem to be very specific (Memory, Real-time…).

What if I say it is possible to model many Linux subsystems, to auto-generate code from the model, to run the model on-the-fly, and that this can be as efficient as just tracing?

- No way!

Yes! It is! It is hard to believe, I know.

In this talk, the author will present a methodology based on events and state (automata), and how to model Linux' complex behaviors with small and intuitive models. Then, how to transform the model into efficient C code, that can be loaded into the kernel on-the-fly to verify Linux! Experiments have also shown that this can be as efficient as tracing (sometimes even better)!

This methodology can be applied on many the kernel subsystems, and the idea of this talk is also to discuss how to proceed towards a more formally verified Linux!

I agree to abide by the anti-harassment policy

Yes

Primary author: BRISTOT DE OLIVEIRA, Daniel (Red Hat, Inc.)

Presenter: BRISTOT DE OLIVEIRA, Daniel (Red Hat, Inc.)

Session Classification: LPC Refereed Track