Discussion Part 1: Identifying internal stage compositions

Instrumentation

Participant

So the instrumentation does influence some of the different stages later on, so there's no connection to the initial seeds. I can quite easily separate these two tasks and only these are should be separately considered. However, if I have to search strategy where I choose one of the seats I have in my queue, this is truly influenced by the instrumentation, because instrumentation gives me the feedback or can't provide the feedback so that I can have a more precise search strategy. So without instrumentation, the search strategy really degenerates if I don't have any feedback from that, I'm degenerating to black box fuzzing or more or less. So this is quite obviously.

And power schedule, I wouldn't say that it's connected to the instrumentation. It's more on the higher level.

The execution should be also connected to instrumentation.

But as the instrumentation is in the executable binary we have which we have later on, it does influence execution, but we can see and how fast it is and stuff like that. So this is trivially in my opinion.

Initial Seeds

Participant

I think it's quite orthogonal to all other half stages. I'll talk a little so.

It's somewhat a separate, so if you if you try to find the correct seeds to start somewhere, I mean it's connected to the search strategy more or less. But if I want you to evaluate, it's usually I would have to manually add both: so if I have different site strategy and a different seed strategy, obviously I need some different visualization. But if I just change the initial seeds and consider like the search strategy unchanged. This doesn't really it a lot.

In the end, I would like to compare the initial seeds to the seeds I get later on maybe.

So if I if I have a different point of time, I do have my different seats and.
If I want to yeah, just check the quality of the corpuses would be more like, I guess that's the point you would consider, like, what individual seeds lead to which different corpus at that point of time after I don't want.

Search Strategy

Participant
I do know the expression seed selection which is, I guess you'd the search strategy. If I remember correctly from above.

Yeah, this is strongly connected to the power schedule in my opinion.
Because if I have different power schedules, different search strategies makes sense and it's connected to that. Like if I change the search strategy, there might be different schedule needed for that.

Is also connected to the mutations to selection which mutation should be applied.

Power Schedule

Participant
Yeah, the poor schedules does influencing the mutations.

I'm just thinking about the relationship between initial seeds and power schedule.
You obviously could have different power schedules for the initial seats, which might make sense. So initial seats are hand selected usually are generated beforehand before the fuzzing. Does all this different stuff so.

Mutations

Participant
What mutations influence execution.
The influence of search strategy, as mentioned earlier.

Execution

Participant

Execution is influencing the power schedule.

Interviewer

Could you maybe explain this part a bit? Why do you think so?

Participant

Well, if I change the execution, right? So if I have a different execution of that stuff and I have different run types and stuff like that, I might want to check like what power schedule is on and how should I change that power schedule to allow? A different energy, so different stuff to have, so executions nevertheless unchanged and stuff like that.
Do I need to adopt the power schedule for different execution?

Yeah. And execution also has relationship to the mutations. I mean the best example for that is red queen, right if I run an execution to some point to where I see, OK, I do have compare stuff like that. So I will change based on this execution, I will have different mutations.

Interviewer

Just because you mentioned filtering before.
I would also ask you if you can do to the same kind of mapping to the stages.

Participant

Is connected to search strategy, I mean it's like a pre-sorting step more or less. It might be like you have different but really influences like what can I look into later on and which can I select?

Interviewer

Alright, you can also tell me the other way around, so if something else on the right influences filtering because we did not do it before.

Participant

Filtering and mutations or more or less mutations and filtering. For example, if I have some mutations which are always filtered out which never lead to something interesting in that sense, this is connected. I'm trying to think of which direction this would be. It's probably from mutations to filtering I guess.

Power schedule is also connected to the filtering and in sense that what influence does a power schedule have like? If I use more or less power for one or the other just results to more or less filtering and stuff.

Discussion Part 2: Identifying visualization analysis tasks

Instrumentation

P4.1 AT. How does the instrumentation the execution speed? Application-level fuzzing vs IoT fuzzing

Participant

How does the instrumentation affect the execution speed. It's definitely something you know, it's which is always considered as a fuzzing, can only be so. So if I have a lot of different executions per second, especially if we move from the, more high level application level fuzzing to the IoT and stuff, fuzzing where you do have if you have bad luck only like 10 executions per second or one executions per 10 seconds.

P4.2 AT. Does instrumentation improve the detecting of bugs?

Participant

Improve the detection of bugs is probably the most important part of instrumentation. If, especially if I'm not only considering the instrumentation of the fuzzer.

P4.3 AT. Does instrumentation change with selected seeds?

Participant

Does instrumentation change with which seeds are selected for further mutations, so the connection between the segmentation and search strategy.

It's a bit hard to do that obviously because it's a different seeds if you have different, so different inputs, sorry, but I guess it's something you would want to tackle.

P4.4 AT. Does instrumentation help cover different parts of the target?

Participant

The instrumentation lead to different parts of the target being reachable or being covered more or less. In general, obviously, if you have more coverage, it's Nice, but if you have only more coverage in the same functions, this might be less interesting. And if you can get into more nice stuff such as you get past crypto or stuff like that. It's probably more interesting.

Initial Seeds

P4.5 AT. How does derived seeds compare to the initial ones at different time points?
P4.6 AT. What kind of head start does the initial seeds provide when compared to empty seed?

Participant

What kind of head start does the seed giving me if I compare it to an empty seed? Like if I start with the empty seat is what if you consider the example of AFL which was quite popular that AFL was correctly inferring the? I think it was the PNG File format and showed here it was able to do that and the question is there like if I compared if the initial seat was already PNG would that be like any difference in the end after 24 hours or to reach the saturation earlier on so?

Participant

This might only be something from resources safe, but not more interesting parts.

P4.7 AT. How does the coverage vary between different initial seeds in the target when compared to each other?

Participant

I would like to see like the distribution of coverage in the target between the different initial seats. So for example, if I take libtiff stuff like that, so I have different formats and codecs and stuff like that. There reach different parts of the library because different parts of the library deal with the different formats. So this might be like the difference with initial seeds and how does this perform? Coverage heat map, which is usually what I use for that.

Do you know, fuzz introspector?

Interviewer
Yeah, they have a UI as well where they show which branches are covered, which code, what's the code covered. I think they also provide call graph information.

Participant
They have a call tree. I think modest. So they have tried to identify blocking, blocking, yeah. Blocking factors. First blocker, we have the father isn't getting past and conditioner or stuff like that. So they consider like, how is this executed? And they have like a huge diagram where for each line of code or each core more or less there's a color coded information. If it's this was hit a lot of times or this was never hit or just like a few stuff, but I think this is like just like what I would see here for the coverage as well to have something like OK and this coverage is getting into this part.

P4.8 AT. How does the initial seeds relate to the changes to the strategy?
P4.9 AT. What parts of the initial seeds are considered interesting?

Participant
How does? Well now the interesting part is also like how does the initial seeds change the search strategy? Or what is the is it? Does it change which seats are selected?
Like if there's like one initial seed or so, if I have different initial seats for in the end, only one of those is really interesting and really useful. It like what parts of the initial seats are actually.

Search Strategy

P4.10 AT. Was the seed selected often enough to reach the interesting behavior ?

Participant

I don't have a lot of different experience with the search strategy. I am really wondering how I would evaluate it and would like to have some visualization.

To see strategy also like if one of the parts is covered more in depth or stuff like that. So in the end, you also want to know like even though I covered the vulnerability that I reach the true conditions for that. So was the seat selected often enough that I could perform all the different mutations, especially if I've randomized mutations and don't have a generative mutation schedule stuff like that.

P4.11 AT. Is search strategy is biased to mutations?

Participant

That's the mutations and such strategy because if only seeds of the same could draw were generated by the same mutation, stuff like that, that would be quite interesting. So if this set strategy is biased towards one or other mutations. I'm not quite sure if that fits here better or for the mutations part.

P4.12 AT. Does the strategy work better with power schedule A or B ?

Participant

That's the search strategy works, but with power scheduler a A or schedule B.

Power Schedule

Participant

Haven't thought about that a lot too, and this is really internal stuff and more you think about usability and what kind of results you're getting at. I can't really think a lot about what you want to you to see here?

Interviewer

Do you want take a bit more time or should we move on to the next one?

Participant

I think we can move on.

Mutations

P4.13 AT. Comparison between different mutation strategies - coverage, bug conditions

Participant

So obviously, does mutation A lead to more new coverage the mutation B does mutation?

Does mutation A more successfully trigger bug error conditions? So again the difference between reaching and triggering a bug.

P4.14 AT. Does mutation A lead to new path with time?

Similar like what we are seeing in Red Queen does mutation A lead to new paths covered in shorter time so.

Not in shorter time but more successfully in the sense that even though I have randomized mutations, I might clear a magic bytes test, but, I guess if I have specialized mutations for that I'm getting more parts or some blockers and stuff like that.

Participant

I think we already have said, early on in this uh search strategy where we do have the connection between the mutation. So I guess it's covered here again.

P4.15 AT. Mutations compare with execution speed and execution resource consumption?

Participant

So for the mutation - execution there's, If I have some mutations which I might be quite useful but really slow down the execution, needs to be put into perspective, I guess so.

How does the mutation influence execution speed? and execution resource consumption.

P4.16 AT. Do I need less mutations with a strategy when compared to another with a trade off to execution speed?

Participant
Do I need less execution with this mutation to get to that same coverage more than so if I have smarter mutations I might slow down the execution, but in the end I get the same results.

Execution

P4.17 AT. Does filtering change seed selection in search strategy?

Participant
Does filtering change which seeds are selected is the obvious one, so.
It might be the case that the seeds which are filtered out might never be seen the selected for a seed later on, even though there would be a seed but maybe can seed change the overall population and thus change the seat selection, so there might be some side effects of that that would be probably interesting.

P4.18 AT. Does energy assignment reduce or increase filtering of mutants?

Participant
I have a different power schedule assigned different power to one seed. This might lead to the seed being on the more filtering or set stuff because it didn't give him enough time and power. The question would be in essence, this energy assignment reduce or increase filtering of mutants.

P4.19 AT. Does the filtering biased towards some mutations?

Participant
And you know the last part of mutations and filtering is again there's that's the filtering always or is it filtering bias towards mutation so that some mutations are always filtered out or some mutations? Not that mutation self, but the seeds or inputs which were gathered by those mutations. That is different and it's also connected with the search strategy.

P4.20 AT. Does changes in execution perform different between power schedules?

Participant
Do the changes in execution require to perform different for different power schedules.
So there might be some side effects as well, where we do have the executions improving a bit, but it's only true for one schedule. But if I have a different schedule, this might change.

P4.21 AT. Does changes in execution perform different between mutations? Biasing?

Same towards mutations. Different mutations might eat, might have different. Executions requirements or change the execution. I might be biased towards one or the different mutations.