Discussion Part 1: Identifying internal stage compositions

Instrumentation

Participant
My point of view, instrumentation is related to power schedule/fitness function.

The fitness function is directly calculated from the things that you observe and the observation is based on the instrumentation. So, for example likes to monitor the coverage, but your instrumentation provides you the information for each taken function or something and not for each basic block.
So let's say for each function just but you don't have no idea which part of this function was is it was executed, so you will also get less information in order to have a good fitness function.

I should also connect this and the instrumentation is for sure also related to the execution because without execution you will not get any information about the instrumentation.

Initial seeds has no relationship because it's independent.
Search strategy is also independent from the instrumentation. Mutation is also independent. It's dependent from the from the fitness function.
Yeah.

Initial Seeds

Participant
Initial seed is also what I found most interesting and how the relationship between initial seeds and mutation is.
I think the most important one is the relationship between initial seed and the mutation. For example, executing Fuzzer A with different seeds and just see if how they perform because depending on the initial seed, you can have better or worse performance.

I will also connect initial seeds the search strategy.

So instrumentation is not. Yeah, there's no relationship between. It's separate.

There is also a relationship to let's make it like this to this power schedule because, the initial seed will also get some fitness function, so there is a relationship between them.

So there's a relationship between this fitness function and execution.
But I think there's no direct relationship between initial seed and execution.

Search Strategy

Participant
Search strategy is for sure, related again to the fitness function because, the seeds or the inputs that had the better fitness function within probably depending on how the search strategy selects the seeds for the new iteration.

You have also a relationship to mutation because only this one that will be selected also mutate.

And a relationship between the initial seed because you will select at the very beginning some of the initial seed.

There's also this relationship between search strategy and the instrumentation because based on what you discovered maybe your search strategy performs better or worse. So yeah, if you're interested in which one is buffer access to memory, then maybe you're strategy is based on, which one is a better access to the buffer overread or something. So depending on that I think there is a relationship between the instrumentation and the search strategy and because this is the main focus: how and what you like to observe; what you observe based on the instrumentation.

Power Schedule

Participant
Previously you have this relation between fitness function and instrumentation. So just what you instrumented and can observe can be affected the fitness.

Relation between yeah fitness function and search strategy.

I will not add this relationship between power schedule and mutation because it's more like indirect through the search strategy.

Mutation

Participant
Exactly so mutation is related to initial seed, it's related to search strategy.

It's not related to instrumentation because it's independent of what you have instrumented.

It's also independent of the execution.

It should be also independent from the power schedule: so I was just thinking about because there are fuzzers in the literature which perform crossovers. So when you have two inputs and, then you take one part of the one input and the second part of the other one, or also in between some exchange. Yeah, so splicing and crossovers are the same.

Read the paper where they just splice with inputs. It had better fitness or better energy. So in this way, if you have such a fuzzer or such an approach, then it's the mutations also related to the power schedule because you did not splice with all of the other inputs, but just take specific ones into account, so this may be good (good energy or good fitness.)

Execution

Participant
Execution is related to Instrumentation because when you execute it, you can just or yeah maybe the other way around to instrumentation is use this when you do not execute the syncs that you have instrumented. So yeah, this the relation there and

You have the relation with power schedule because after the execution you can just see what you have executed with this input and then give this energy from the fitness function to it.

There's no relationship between mutation and execution.

Search strategy, I would also say there's no.

Initial seeds are also independent.

Discussion Part 2: Identifying visualization analysis tasks

Instrumentation

P6.1 AT. What will be observed during execution?

Participant
I don't know if this is the way you like to have this test, but so first I had this question in mind. OK, what is instrumented? So what would be observed during the execution?

P6.2 AT. How did the instrumentation affect the original SUT?

What is instrumented? So how did I affect the original SUT?

P6.3 AT. What is the effect of instrumentation on the fitness function or energy calculation?

So I was thinking about what was the effect of the instrumentation that affects the fitness function or the energy?

How does the instrumentation affect the energy calculation?
Is also a little bit related to the execution.

P6.4 AT. Filter the instrumentations by type - code coverage, data coverage, etc. What is the effect of each instrumentation type?

What will be also interesting is if you can filter the instrumentations. So I know if you have instrumentation for code coverage and you have other instrumentation for data coverage or something and then you can see, okay, when we just take the code coverage into account. what was the effect of the code coverage instrumentation and what was the effect of the other instrumentation that we did? So yeah, when you have multiple different kinds of instrumentation so that you can in this visualization filter them.

Initial Seeds

P6.5 AT. How does initial seeds are computed? Grammar? Expert knwoledge?

Participant
Yeah, initial seed there. The first question would be how does initial seed are determined? Are they some inputs, from a grammar, are they somehow have a previous knowledge of an expert. So yeah, where does initial seed are coming from?

P6.6 AT. How does initial seeds affect the fuzzing process?

How does the initial seed affects the whole fuzzing process? So yeah, having the same run was maybe also the exact same mutations and, but just different initial seeds. How this affects the whole fuzzing process?

P6.7 AT. What is the effect of initial seeds to their mutants/mutations? How does the initial seeds - mutations decision affect ?

And also the effect of the initial seeds to the yeah, the things that are selected and then mutated afterwards.

P6.8 AT. Would search strategy have different effect with different seed sets?

Oh, how would is another search? Yeah. Would another initial seed then for by the search strategy have a different effect to the next iterations? So yeah, we'll other things be selected and then maybe there are just one or two seeds that were then additionally passes the search strategy and then have a huge impact to the whole fuzzing process, so this would be interesting to check.

P6.9 AT. How does each seed affect fuzzing process?

The effect of also single individuals in this initial seed. So how does a single seed affects the whole fuzzing process?

Search Strategy

P6.10 AT. What is the search strategy?

Participant
So search strategy.
Yeah, there it will be interesting. First, what is the search strategy? So maybe if you use a fuzzer, then if it's somehow possible to without really taking a look into the code to have an basic understanding of, okay, what is the search strategy?
It's often this is always the 10 the 10 seeds was the best fitness or something like this, so have a better understanding how the search strategy is look.

P6.11 AT. How does search strategy affect fuzzing process? with different search strategies?

Yeah, somehow the same question like for the initial seeds how the search strategy affects the whole fuzzing process?
Again, same initial seeds, same mutations, but just different strategy. What will be the effect on the whole puzzle process?
And maybe also not affect just on how good the code coverage or the bug coverage is, increase it but also the performance.

So maybe, I don't know, with a different search strategy, you have to execute 20% more but have at the end the same code coverage so more like in a energy consumption or time consumption, so you execute less test and have at the end the

same code coverage or bug coverage or whatever you had.

P6.12 AT. For each iteration which mutant was selected? Mutant lineage?

So this would be also an interesting.
Yeah, search strategy and mutation. Could be also interesting more from a debugging point of view to see for each iteration of which one was selected so that you can always see for different iteration of the loops, okay, and what was the seed pool at the very beginning and then from the search strategy which one are left over and was used for the next mutations.

Power Schedule

P6.13 AT. What is the effect of the instrumentation to the power schedule?

Participant
Yeah, there it's the same like for instrumentation. So what is the effect for of the instrumentation to the power schedule and also?

P6.14 AT. How does power schedule affect search strategies?

Yeah, I think that's again also the same or things that I already mentioned for the search strategy. How would this power scheduling, energy or the fitness that each individual gets, How this is affecting the search strategy because, based on search strategy some individuals have a lower energy than other ones but still have a good one. They are filtered out.

Let's say your search strategy, okay, always take the 10 best but then the 11th one that also had a very good fitness, but it was not under the ten. So, the other ten was better. So it will filter out. And what is the effect then?

Yeah. So this relationship would be also nice to somehow, from a debugging point of view to check, okay, what was left over just because of the search strategy.

Mutations

Participant
For the mutations, we had this relationship to initial seed already at the beginning.

Interviewer
I think in the beginning it was the other way around. Now it's from mutations to initial seeds.

P6.15 AT. What kind of mutation strategies were performed?

Participant
So yeah, I think the mutations.
The initial seeds had the effect on the mutation.
So I had this question at the very beginning.
So I think what would be also interesting for the internal stage is for sure what kind of mutations will was performed.
Like AFLGo, I think they have multiple different kinds of mutations they will perform and then based on.
Yeah, based on some information they depend more or less.
Depending on this, an AFA going function, but yeah the technical details. So yeah, this would be a nice to have a visualization for that.

P6.16 AT. Which mutations were applied on the concrete test input(s)? Tracing all the mutations

Also, maybe really on the concrete test input, so if you really have this data, for example you have. I don't know. Let's say it's a string. Did you just enter string to the SUT and now If you can just trace OK on which iteration what mutation was made to one individual.

For example the 1st letter always change, but the rest it's just always the same. Then you can just trace over the time. OK how does, initial seed was mutated at so that at the end you have the input that triggers the bug or something or that was this the one who had the most the highest coverage. So I think like tracing all the mutations that would be nice for internal visualization of the stage and I think for the

relationship it's the things that I have already mentioned in the in the previous boxes. So I think we can.

Execution

P6.17 AT. What has changed in the SUT in Execution, when compared to the original SUT?

Move on to the execution.
Yeah, I'm for execution. I think it would be interesting.
Again, a little bit. What was the effect based on the instrumentation? I yeah, we had it also at the very beginning.
But now maybe more like a former SUT point of view. So.
What has changed because there is now the instrumentation in it.
For example, when the instrumentation is affected, the the SUT is running as slower, much lower, and maybe it's something that is.
Really time critical? Then it has a huge effect to the to the whole SUT. So something like this would be interesting.
What was the effect of instrumentation to the execution itself?

P6.18 AT. How energy is varied based on the different execution information? How was the energy calculated?

Interviewer
Execution to power schedule. Can you think of something there?

Participant
Yeah, based on the execution, you will have the information that you observe that the stand useful for the power schedule.
You can also add that maybe it is nice to see what was observed during the execution which then maybe also the formula which was used for the calculation of the power schedule so that you can, have a better tracking to see, OK, this was the information you had doing the test execution and then with this formula this power schedule at the end a value of 7 and nobody knows where the seven is coming from. So you can trace it a little bit better the whole calculation and all the observation it had during execution.