

How to present software analysis results that are conditioned on the software's configuration

Rafael Toledo, Ramy Shahin, Robert Hackman,
Ramesh S, Joanne M. Atlee, Marsha Chechik

Outline

- Our research group is working with GM researchers on next-generation program analysis tools (specializing in reporting system-wide dataflows and component interactions).
- Our analyses can accommodate configurable software and report analysis results conditioned on configuration settings.
- Demo/presentation + feedback survey should not take more than 1 hour
 - Presentation (+ demo) (15-30 minutes)
 - Survey (15-20 min)

Consent

- Do you agree to participate?
- Do you agree to allow your survey answers to be used in teaching, scientific presentation and/or publications?
- Do you agree to the use of anonymous quotations in any presentation or publication that comes from this research?

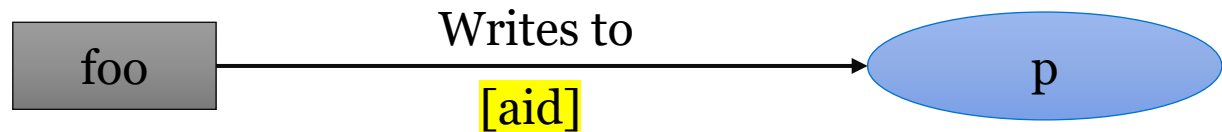
You may withdraw from the study (and leave the presentation or survey) at any time for any reason, no questions asked.

Software analysis results conditioned on the software configuration

- Identify patterns in variable code
- Example analyses
 - Data-flow analyses
 - Control-flow analysis
 - Behaviour alteration analysis

```
bool aid; //configuration variable
int p;
```

```
void foo() {
    . . .
    if (aid) {
        p = . . .;
    }
    . . .
}
```



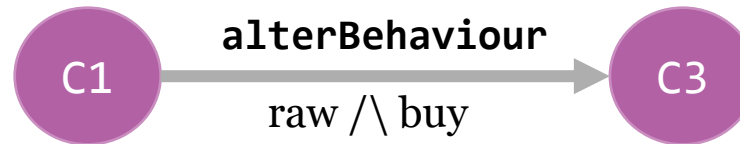
Associate results with configuration expressions

- Analysis results true in some program configurations (variants)
- Annotate results with a configuration expression
- Boolean expressions over configuration variables (e.g., aid, art, buy, raw)
 - Single variant: aid /\ art /\ !buy /\ raw
 - Multiple variants:
 - (aid \/ art) /\ !raw (6 possible variants)
 - !raw (8 possible variants)

Software analysis = query over program elements

- Query language (Cypher)

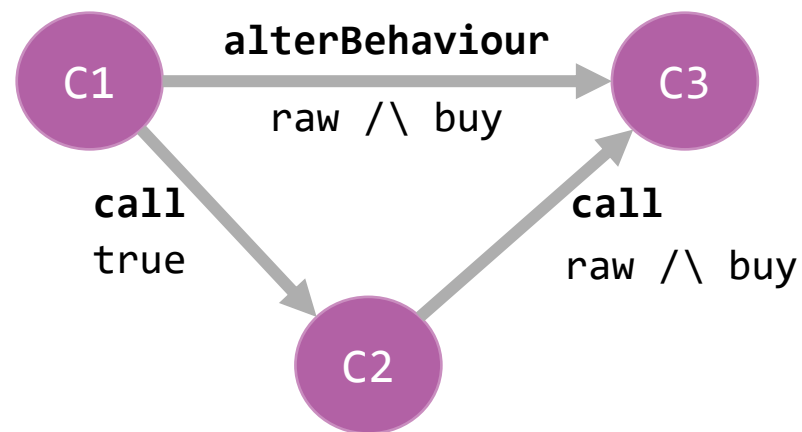
```
MATCH (srcComp)-[:alterBehavior]->(dstComp) RETURN *
```



Software analysis = query over program elements

- Query language (Cypher)
- Querying different details of the graph

```
MATCH (srcComp)-[:alterBehavior]->(dstComp)
MATCH (srcComp)-[:call]->()-[:call]->(dstComp) RETURN *
```

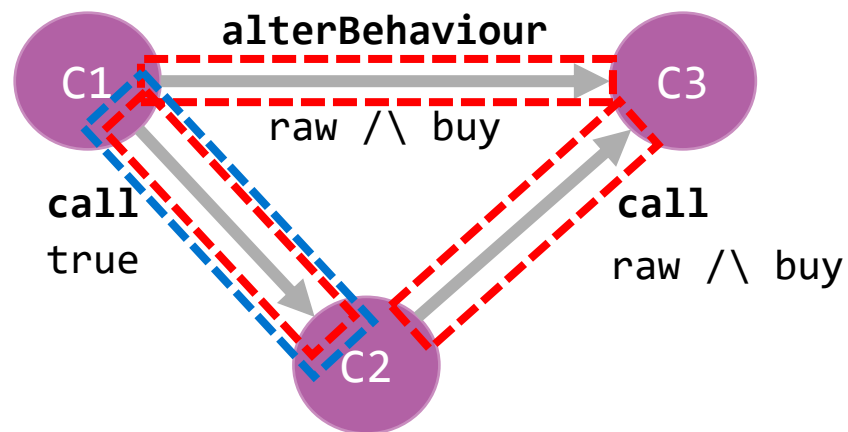


Filtering analysis results

- Identify results that are present in a variant
- Create filters for configuration expressions

V1: raw

V2: raw /\ !buy



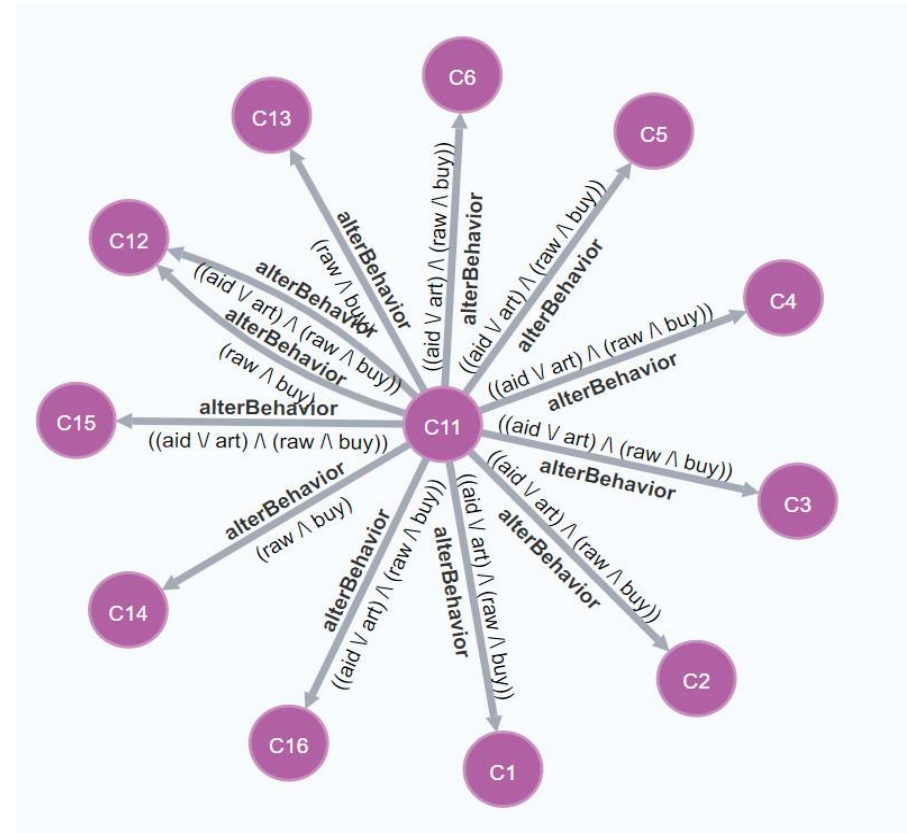
Results format

Behaviour Alteration analysis (path between components)

Tabular

srcComp	dstComp	behaviourAlterationEdge
C11	C13	$\text{raw} \wedge \text{buy}$
C11	C12	$\text{raw} \wedge \text{buy}$
C11	C6	$(\text{aid} \vee \text{art}) \wedge (\text{raw} \wedge \text{buy})$
C11	C12	$(\text{aid} \vee \text{art}) \wedge (\text{raw} \wedge \text{buy})$
C11	C3	$(\text{aid} \vee \text{art}) \wedge (\text{raw} \wedge \text{buy})$
C11	C15	$(\text{aid} \vee \text{art}) \wedge (\text{raw} \wedge \text{buy})$
C11	C5	$(\text{aid} \vee \text{art}) \wedge (\text{raw} \wedge \text{buy})$
C11	C14	$\text{raw} \wedge \text{buy}$
C11	C2	$(\text{aid} \vee \text{art}) \wedge (\text{raw} \wedge \text{buy})$
C11	C16	$(\text{aid} \vee \text{art}) \wedge (\text{raw} \wedge \text{buy})$
C11	C1	$(\text{aid} \vee \text{art}) \wedge (\text{raw} \wedge \text{buy})$
C11	C4	$(\text{aid} \vee \text{art}) \wedge (\text{raw} \wedge \text{buy})$

Graphical



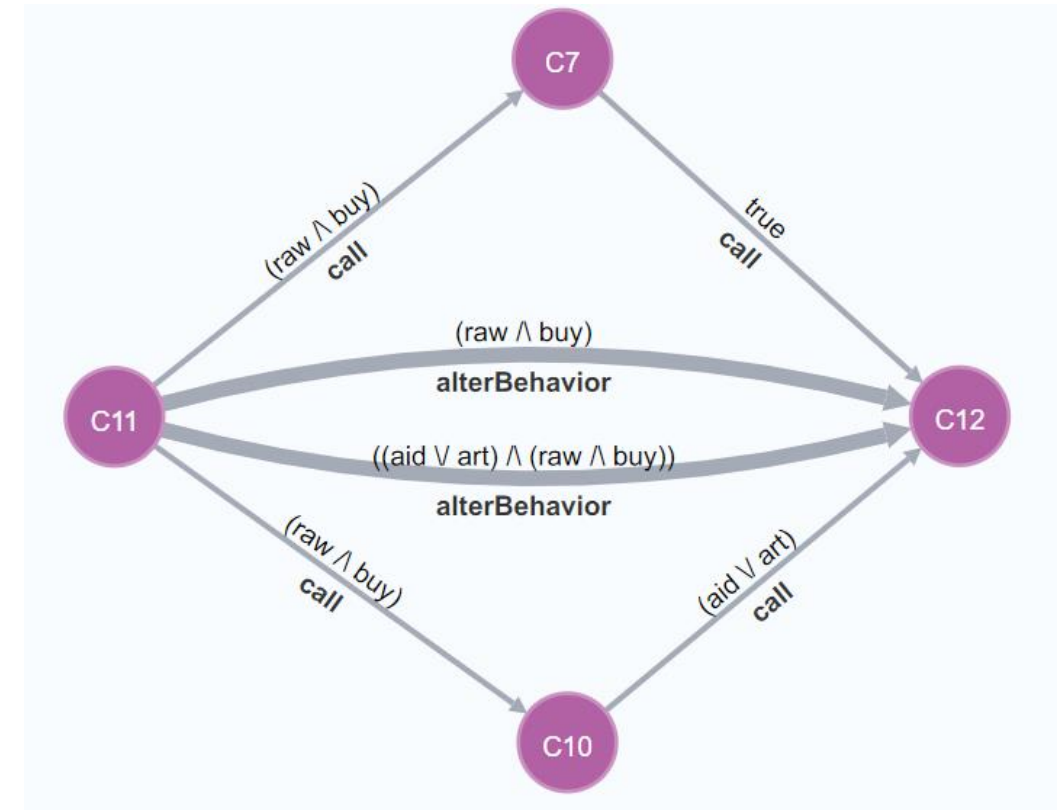
Results format

Behaviour Alteration analysis (with internal calls)

Tabular

relationshipType	srcComp	dstComp	relationshipCondition
call	C11	C7	$(raw \wedge buy)$
call	C7	C12	TRUE
alterBehavior	C11	C12	$(raw \wedge buy)$
call	C11	C10	$(raw \wedge buy)$
call	C10	C12	$(aid \vee art)$
alterBehavior	C11	C12	$((aid \vee art) \wedge (raw \wedge buy))$

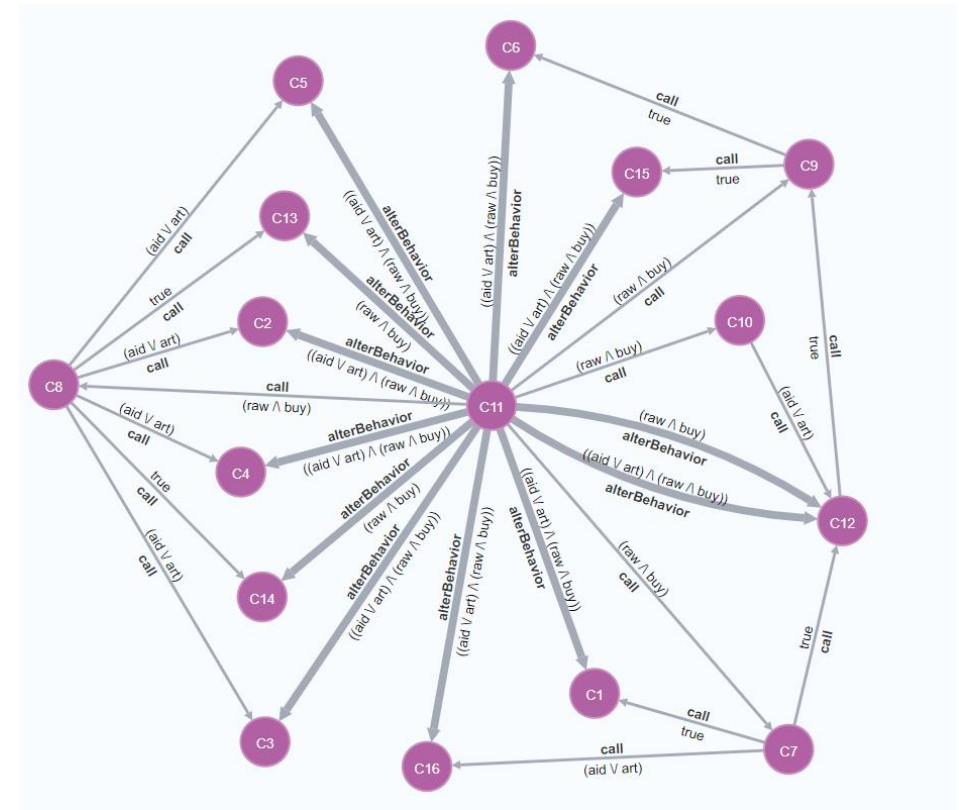
Graphical



Tabular

relationshipType	srcComp	dstComp	relationshipCondition
call	C7	C1	TRUE
call	C7	C12	TRUE
call	C7	C16	(aid \vee art)
call	C8	C14	TRUE
call	C8	C3	(aid \vee art)
call	C8	C13	TRUE
call	C8	C2	(aid \vee art)
call	C8	C4	(aid \vee art)
call	C8	C5	(aid \vee art)
call	C9	C6	TRUE
call	C9	C15	TRUE
call	C10	C12	(aid \vee art)
call	C11	C8	(raw \wedge buy)
call	C11	C9	(raw \wedge buy)
call	C11	C7	(raw \wedge buy)
call	C11	C10	(raw \wedge buy)
call	C12	C9	TRUE
alterBehavior	C11	C13	(raw \wedge buy)
alterBehavior	C11	C12	(raw \wedge buy)
alterBehavior	C11	C6	((aid \vee art) \wedge (raw \wedge buy))
alterBehavior	C11	C12	((aid \vee art) \wedge (raw \wedge buy))
alterBehavior	C11	C3	((aid \vee art) \wedge (raw \wedge buy))
alterBehavior	C11	C15	((aid \vee art) \wedge (raw \wedge buy))
alterBehavior	C11	C5	((aid \vee art) \wedge (raw \wedge buy))
alterBehavior	C11	C14	(raw \wedge buy)
alterBehavior	C11	C2	((aid \vee art) \wedge (raw \wedge buy))
alterBehavior	C11	C16	((aid \vee art) \wedge (raw \wedge buy))
alterBehavior	C11	C1	((aid \vee art) \wedge (raw \wedge buy))
alterBehavior	C11	C4	((aid \vee art) \wedge (raw \wedge buy))

Graphical



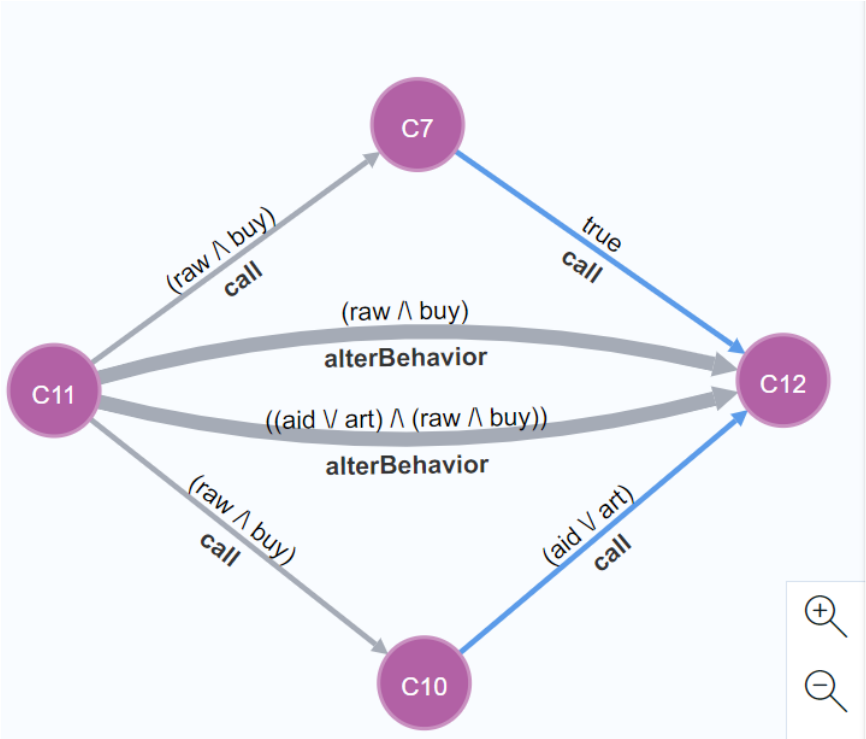
Results filtered by a single variant (small example)

aid /\ art /\ !raw /\ buy

Tabular

relationshipType	srcComp	dstComp	relationshipCondition
call	C11	C7	(raw /\ buy)
call	C7	C12	TRUE
alterBehavior	C11	C12	(raw /\ buy)
call	C11	C10	(raw /\ buy)
call	C10	C12	(aid \/ art)
alterBehavior	C11	C12	((aid \/ art) /\ (raw /\ buy))

Graphical



Filters
aid /\ art /\ !raw /\ buy
Displaying 4 nodes, 6 relationships.

Results filtered by two variants (small example)

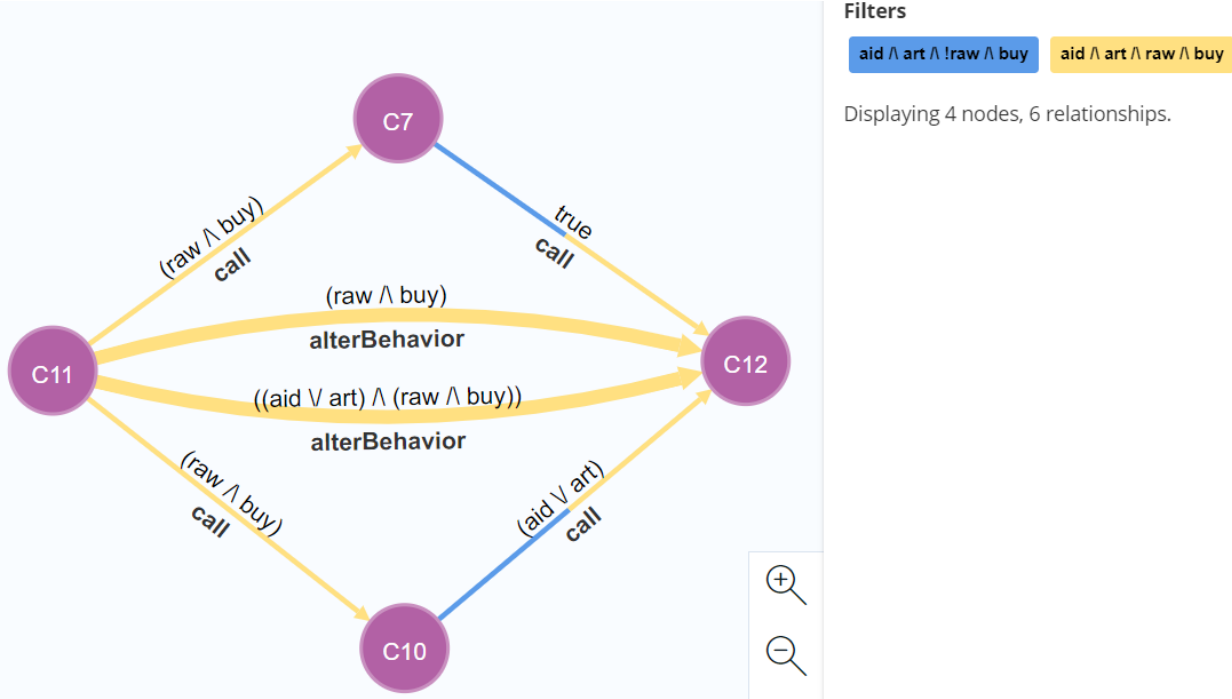
aid \wedge art \wedge !raw \wedge buy vs.

aid \wedge art \wedge raw \wedge buy

Tabular

relationshipType	srcComp	dstComp	relationshipCondition
call	C11	C7	(raw \wedge buy)
call	C7	C12	TRUE
alterBehavior	C11	C12	(raw \wedge buy)
call	C11	C10	(raw \wedge buy)
call	C10	C12	(aid \vee art)
alterBehavior	C11	C12	((aid \vee art) \wedge (raw \wedge buy))

Graphical



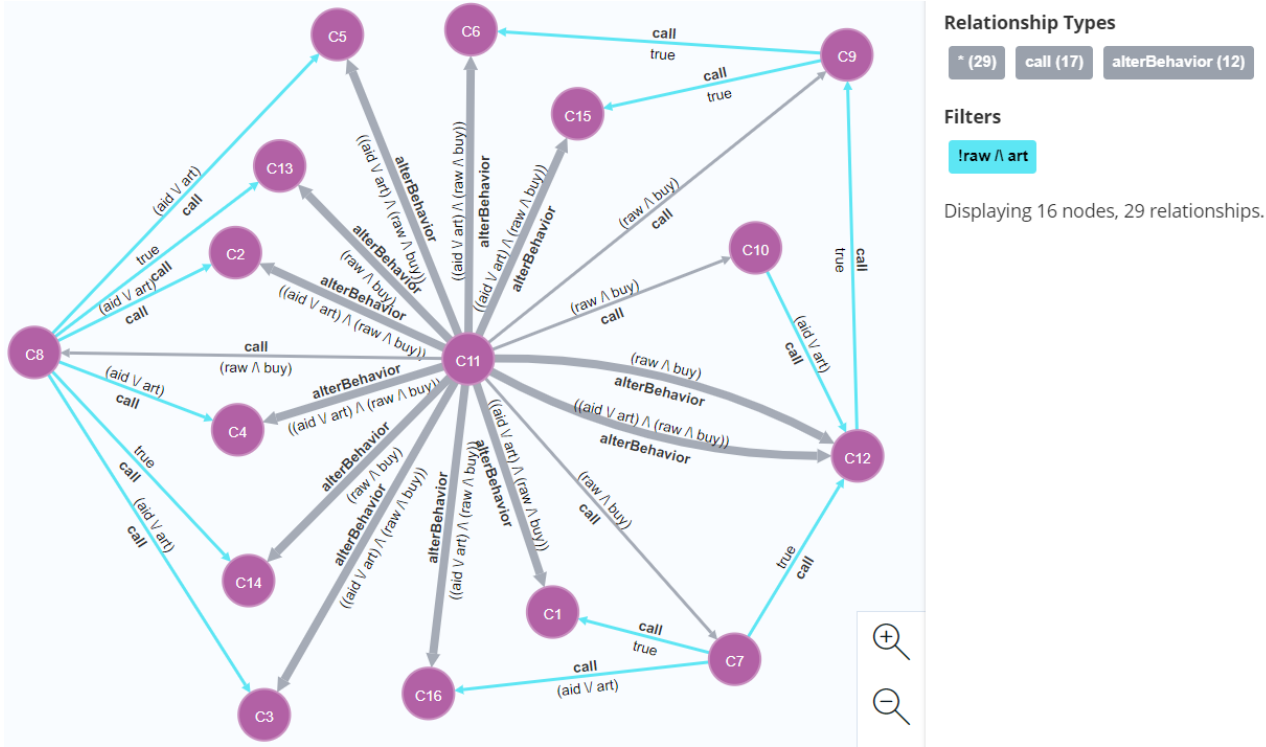
Results filtered by a group of variants

!raw /\ art

Tabular

relationshipType	srcComp	dstComp	relationshipCondition
call	C7	C1	TRUE
call	C7	C12	TRUE
call	C7	C16	(aid ∨ art)
call	C8	C14	TRUE
call	C8	C3	(aid ∨ art)
call	C8	C13	TRUE
call	C8	C2	(aid ∨ art)
call	C8	C4	(aid ∨ art)
call	C8	C5	(aid ∨ art)
call	C9	C6	TRUE
call	C9	C15	TRUE
call	C10	C12	(aid ∨ art)
call	C11	C8	(raw ∧ buy)
call	C11	C9	(raw ∧ buy)
call	C11	C7	(raw ∧ buy)
call	C11	C10	(raw ∧ buy)
call	C12	C9	TRUE
alterBehavior	C11	C13	(raw ∧ buy)
alterBehavior	C11	C12	(raw ∧ buy)
alterBehavior	C11	C6	((aid ∨ art) ∧ (raw ∧ buy))
alterBehavior	C11	C12	((aid ∨ art) ∧ (raw ∧ buy))
alterBehavior	C11	C3	((aid ∨ art) ∧ (raw ∧ buy))
alterBehavior	C11	C15	((aid ∨ art) ∧ (raw ∧ buy))
alterBehavior	C11	C5	((aid ∨ art) ∧ (raw ∧ buy))
alterBehavior	C11	C14	(raw ∧ buy)
alterBehavior	C11	C2	((aid ∨ art) ∧ (raw ∧ buy))
alterBehavior	C11	C16	((aid ∨ art) ∧ (raw ∧ buy))
alterBehavior	C11	C1	((aid ∨ art) ∧ (raw ∧ buy))
alterBehavior	C11	C4	((aid ∨ art) ∧ (raw ∧ buy))

Graphical



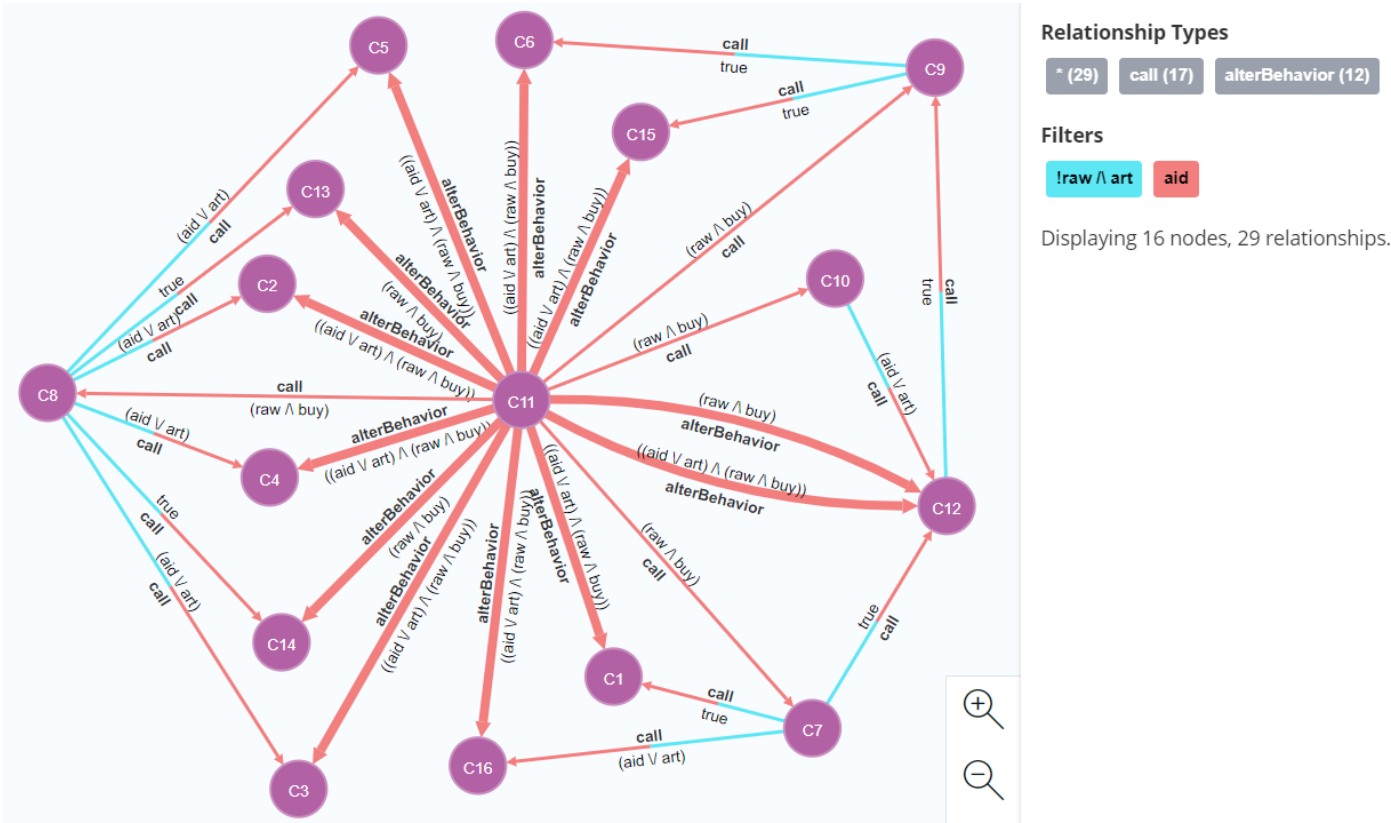
Compare groups of variants

!raw /\ art vs. aid

Tabular

relationshipType	srcComp	dstComp	relationshipCondition
call	C7	C1	TRUE
call	C7	C12	TRUE
call	C7	C16	(aid \vee art)
call	C8	C14	TRUE
call	C8	C3	(aid \vee art)
call	C8	C13	TRUE
call	C8	C2	(aid \vee art)
call	C8	C4	(aid \vee art)
call	C8	C5	(aid \vee art)
call	C9	C6	TRUE
call	C9	C15	TRUE
call	C10	C12	(aid \vee art)
call	C11	C8	(raw \wedge buy)
call	C11	C9	(raw \wedge buy)
call	C11	C7	(raw \wedge buy)
call	C11	C10	(raw \wedge buy)
call	C12	C9	TRUE
alterBehavior	C11	C13	(raw \wedge buy)
alterBehavior	C11	C12	(raw \wedge buy)
alterBehavior	C11	C6	((aid \vee art) \wedge (raw \wedge buy))
alterBehavior	C11	C12	((aid \vee art) \wedge (raw \wedge buy))
alterBehavior	C11	C3	((aid \vee art) \wedge (raw \wedge buy))
alterBehavior	C11	C15	((aid \vee art) \wedge (raw \wedge buy))
alterBehavior	C11	C5	((aid \vee art) \wedge (raw \wedge buy))
alterBehavior	C11	C14	(raw \wedge buy)
alterBehavior	C11	C2	((aid \vee art) \wedge (raw \wedge buy))
alterBehavior	C11	C16	((aid \vee art) \wedge (raw \wedge buy))
alterBehavior	C11	C1	((aid \vee art) \wedge (raw \wedge buy))
alterBehavior	C11	C4	((aid \vee art) \wedge (raw \wedge buy))

Graphical



Seeking feedback on results representation

- Which format is easier to **read, understand, search, explore**?
- Which format is better to represent **variable results** depending on configuration variants?
- <https://bit.ly/3vOxRS9>