Static analysis

Widely used.
Active area
Papers: case studies.
Google, Facebook

Q: what are specs?

Specs?

Partial/aspects vs. full correctness.
Co-design "spec" vs. write full spec.
Heuristic/"universal" vs. app-specific.
Internal vs. external behavior.
↳ invariant.
Locality vs. whole execution.
Practicality vs. completeness.

Case study: FindBugs @ Google

- Dashboard.
  - Developers ignored.
  - Facebook: 0% fix rate.
  - → ← "Master" bug list
    - ↳ Owned by sec eng team ←
- File bug reports.
  - Not worth fixing.
  - Facebook: "near silence".
  - → ← Sec engineers file bugs.
- Code review. → good plan.
  - FindBugs: too much customization.

sooner

- Compile time.
  - Google: review ⇝ compile-time.
  - Facebook: too slow/costly.

Common themes

"Context switch".
↑ Who fixes it?
↑ Shorter feedback loop

Solve problem for dev/eng.

- Right time.
- Right insight.
- Right dev/eng.

How deal w/ bugs?

→ Testing → unit
→ integration
→ monitoring

→ Runtime checks → races
→ overflows
⋮

Static analysis
∀ exec / ∀ inputs.

↳ security.

↳ mobile devices.

Google: pitfalls, avoidance.

- Developer workflow.
  - Compile-time
  - Review-time
  - File bugs
  - Batch

Facebook ⇒ Google

- Actionable warnings.
  - Legacy code FP.
  - Fix bugs/warnings before deploying tool.
- User trust.
  - Google: avoid FP ≙ action.
  - FB: pick teams/problems.
- Relevant/fixable
- Understand warnings.

```
printf("%s %d %s", x, y, z);
```

Focus/metrics.

Google: "effective false positive". EFP.

Fix nuisance warning ⇒ not EFP

Missed real issue ⇒ EFP.

Flag "not useful".

First lesson: "always bugs".

⇒ Unobjectionable bugs.

FB: "missed bugs".

Q: "How could we have caught it w/ analysis?"

Focus areas:

- Crashes
- Security.
- Concurrency. ←

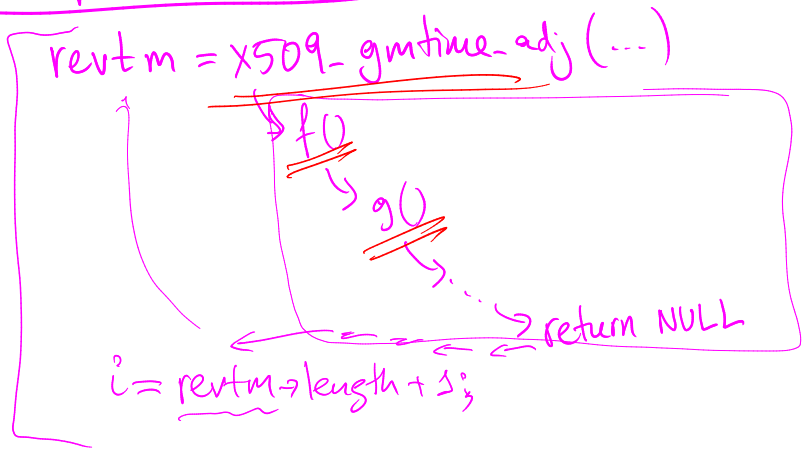
Works well:

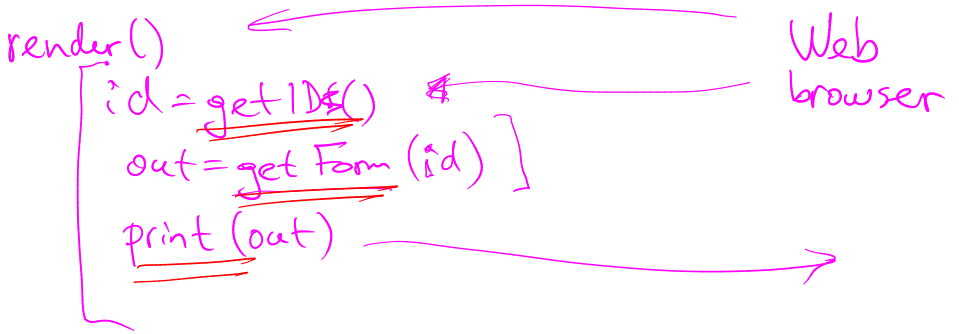
3 data races missed. → 50% false positives.

Devs tolerate FP ↑.

11 see bugs missed. ★★

Interprocedural bugs





Compositional analysis

"Procedure summary": intermediate spec for every func

Who writes intermediate specs?

Infer: deduce specs.

Linux: annotations.