Evaluating how we find bugs

How could an accurate, scalable, convenient bug-finder still embody a relatively ill-advised approach?

Some straw-men to show it's possible:

- Simpler ways to find same bugs
- Simpler ways to avoid the bugs

The base-line for research will increase

Evaluating how we find bugs

```
void f(){
  …
  t x;
  …
  g(&x);
  …
}
```

sophisticated dynamic detection

vs.

simple “insert initializer” transformation

Evaluating how we find bugs

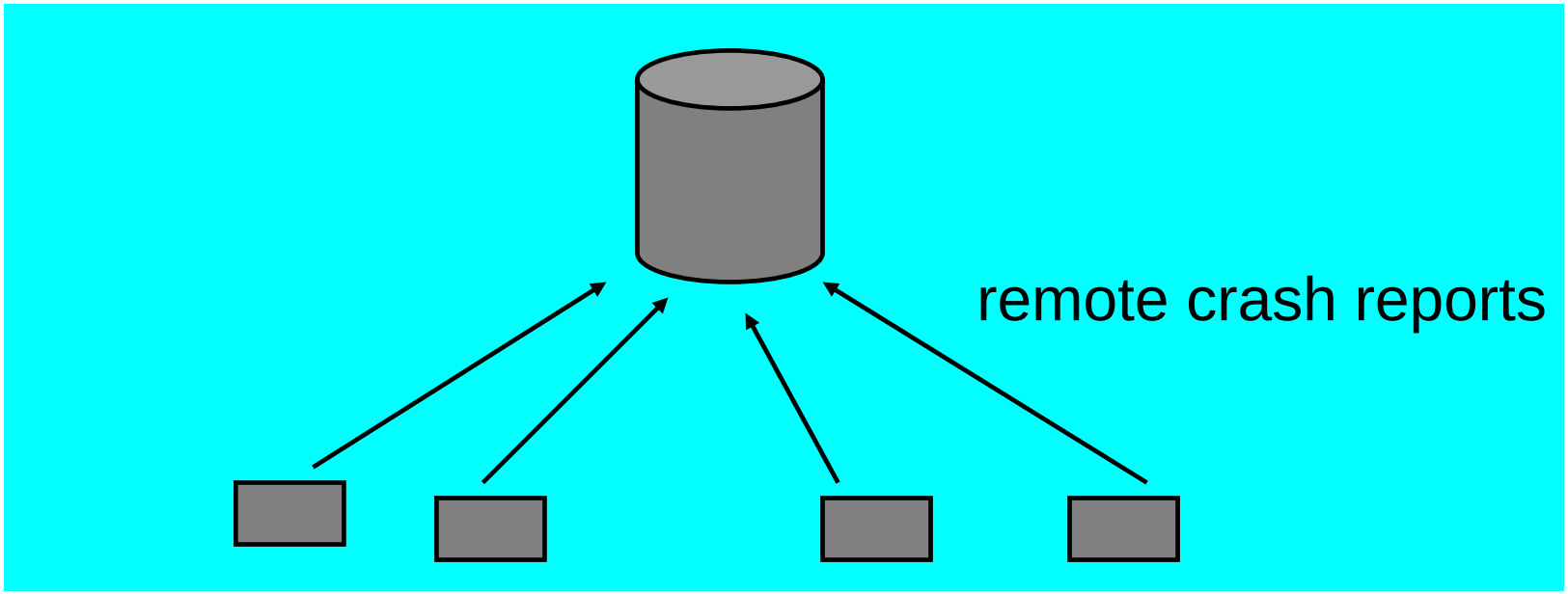
```
void f(){
  …
  free(p);
  …
  free(q);
  …
}
```

analysis useful on some applications

vs.

analysis useful on applications *needing* free

Evaluating how we find bugs



deployment infrastructure finds bugs

vs.

deployment infrastructure *needed* to find bugs