SAFER C, ADDRESS SANITIZER AND FUZZING

```
int main() {
        int a[2]={1,0};
        printf("%i\n",a[2]);
}
```

-fsanitize=address
(gcc, clang/llvm)

Address Sanitizer adds some meory safety.
Prevents most use after free, out of bounds read/write etc.
Significant cost (50-100%), but better than everything that was available before.

Address Sanitizer found hundreds of bugs with fuzzing.
Intended as a Debugging-Tool, but why stop there?

Can we build a system with Address Sanitizer?
Yes, I built Gentoo Linux base system.

Why?

Just doing so uncovers bugs.

May be used as a "safe" Linux for high security requirements.

QUESTIONS?

https://fuzzing-project.org/

https://hboeck.de